Approximating the Number of Irreducible Polynomials over $\mathbb{F}_2$ with Several Prescribed Coefficients

Behzad Omidi Koma and Daniel Panario *
School of Mathematics and Statistics, Carleton University
Ottawa, ON, K1S 5B6, Canada
bomidi,daniel@math.carleton.ca

Abstract

Let $N(n, t_1, \ldots, t_r)$ be the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_2$ where the coefficients of the terms $x^{n-1}, \ldots, x^{n-r}$ are prescribed. Finding the exact values for the numbers $N(n, t_1, \ldots, t_r)$ for $r \geq 4$ seems difficult. In this paper we give an approximation for these numbers. We treat in detail the case $N(n, t_1, \ldots, t_4)$, and we state the approximation in the general case. We experimentally show how good is our approximation.

1 Introduction

Let n be a positive integer. 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 [7] 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 $\mathbb{F}_2$. Yucas and Mullen [13] and Fitzgerald and Yucas [6] consider the number of irreducible polynomials of degree n over $\mathbb{F}_2$ when the coefficients of x^{n-1}, x^{n-2} and x^{n-3} are prescribed. Over any finite field $\mathbb{F}_q$, Yucas [12] gives the number of irreducible polynomials with prescribed first or last coefficient. More recently, Omidi Koma, Panario and Wang [10] consider the number of irreducible polynomials with fixed trace and norm. For an ex-

*The second author is supported in part by NSERC of Canada.

cellent survey paper (up to 2005) on polynomials (irreducible or primitive) with prescribed coefficients, see Cohen [4].

For given $n \geq 4$ and $4 \leq r \leq n-1$ we study the number $N(n, t_1, \ldots, t_r)$ of irreducible polynomials of degree n over $\mathbb{F}_2$ where the coefficients of the terms $x^{n-1}, \ldots, x^{n-r}$ are given as $t_1, \ldots, t_r$. Finding the exact value of $N(n, t_1, \ldots, t_r)$ seems a difficult problem. A conjecture about the number $N(n, t_1, \ldots, t_r)$, for even n, is given in [13]; see also [6]. We give some results about the number $N(n, t_1, \ldots, t_r)$ that allow us to find a good approximation for this number.

We now give the format of this paper. In Section 2 we review the required background and fix the notation. Our main results are given in Sections 3 and 4. In Section 3 we give several results and a formula for the number $N(n, t_1, \ldots, t_4)$ that entails our approximation for this number. We show with concrete examples that our approximation is close to the exact value of $N(n, t_1, \ldots, t_4)$. In Section 4, we first state the formula for the number $N(n, t_1, \ldots, t_r)$ and its approximation, where $r = 5, 6, 7$. We explain how to find the formula for $N(n, t_1, \ldots, t_r)$ for $r \geq 8$, and we give its approximation. Moreover, our experimental results allow us to sligthly tighten Yucas and Mullen [13] conjecture for $N(n, t_1, \ldots, t_r)$.

2 Preliminary results and background

For a given polynomial $f \in \mathbb{F}_2[x]$ of degree n, let $T_k(f)$ be the coefficient of x^{n-k} in f, where $1 \leq k \leq n-1$. By definition, $T_1(f)$ is the trace of the polynomial f. For $\beta \in \mathbb{F}_{2^n}$ and positive integer k, the k-th trace of β denoted by $T_k(\beta)$ is defined as

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

Let $f \in \mathbb{F}_2[x]$, and d be a positive integer. Then the multinomial theorem gives the coefficients of the polynomial f^d. Let $P(n, t_1, \ldots, t_r)$ be the set of irreducible polynomials $f \in \mathbb{F}_2[x]$ of degree n with given $T_k(f) = t_k \in \mathbb{F}_2$, for $1 \leq k \leq r$. Let $N(n, t_1, \ldots, t_r)$ be the number of polynomials in $P(n, t_1, \ldots, t_r)$. We define $P(n)$ as the set of all irreducible polynomials f of degree n over $\mathbb{F}_2$, and $N(n) = |P(n)|$. In [8] it is given that

$$N(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{\frac{n}{d}}.$$

Let $N(n,t_1)$ be the number of irreducible polynomials f of degree n over $\mathbb{F}_2$ with given trace $T_1(f)=t_1$. If n is a positive even integer and $t_1=1$, then in [1] it is proved that

$$N(n,1)=\frac{1}{2n}\sum_{\substack{d\mid n\\ d \text{ odd}}}\mu(d)2^{\frac{n}{d}}.$$

Hence, for the case trace zero we have $N(n,0)=N(n)-N(n,1)$.

Let $F(n,t_1,\dots,t_r)$ be the number of elements $\beta\in\mathbb{F}_{2^n}$ with $T_k(\beta)=t_k\in\mathbb{F}_2$, and $k=1,\dots,r$. Then, $F(n,t_1,t_2)=|\{\beta\in\mathbb{F}_{2^n}:T_1(\beta)=t_1,T_2(\beta)=t_2\}|$, and we also have $N(n,t_1,t_2)=|\{f\in\mathbb{F}_2[x]:f\in P(n),T_k(f)=t_k,\ k=1,2\}|$. For a statement P, we let [P] = 1 if the statement P is true; otherwise we let [P] = 0. In [2] the formula for $F(n,t_1,t_2)$ is given; they use Möbius inversion formula to connect the numbers $N(n,t_1,t_2)$ and $F(n,t_1,t_2)$.

Theorem 1 *Let n be a positive integer. Assume that $a\equiv b \pmod 4$ is shortened to $a\equiv b$. For different $t_1,t_2\in\mathbb{F}_2$ the formulas for $N(n,t_1,t_2)$ can be given as*

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

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

(ii) $$nN(n,0,0)=\sum_{\substack{d\mid n\\ d \text{ odd}}}\mu(d)F(n/d,0,0)-[n \text{ even}]\sum_{\substack{d\mid n,\ \frac{n}{d} \text{ even}\\ d \text{ odd}}}\mu(d)2^{\frac{n}{2d}-1},$$

(iii) $$nN(n,0,1)=\sum_{\substack{d\mid n\\ d \text{ odd}}}\mu(d)F(n/d,0,1)-[n \text{ even}]\sum_{\substack{d\mid n,\ \frac{n}{d} \text{ even}\\ d \text{ odd}}}\mu(d)2^{\frac{n}{2d}-1}.$$

In [13] the number $N(n,t_1,t_2,t_3)$ of irreducible polynomials $f\in\mathbb{F}_2[x]$ of even degree n with prescribed traces $T_k(f)=t_k$, $k=1,2,3$, is given. For odd n, the number $N(n,t_1,t_2,t_3)$ is treated in [6].

Theorem 2 *Let n be a positive integer, and $a\equiv b \pmod 4$ be shortened as $a\equiv b$. Then*

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

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

(ii) $$nN(n,0,0,1) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,0,1),$$

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

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

(iv) $$nN(n,0,1,1) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,1,1),$$

(v) $$nN(n,0,0,0) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,0,0) - [n \text{ even}] \sum_{\substack{d|n,\, \frac{n}{d} \text{ even} \\ d \text{ odd}}} \mu(d)2^{\frac{n}{2d}-1},$$

(vi) $$nN(n,0,1,0) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,1,0) - [n \text{ even}] \sum_{\substack{d|n,\, \frac{n}{d} \text{ even} \\ d \text{ odd}}} \mu(d)2^{\frac{n}{2d}-1}.$$

For even number n formulas for the numbers $F(n,t_1,t_2,t_3)$ are given in [13], and for odd n formulas for $F(n,t_1,t_2,t_3)$ are given in [6].

3 The formula for $N(n,t_1,\ldots,t_4)$

In this section we study the number $N(n,t_1,\ldots,t_4)$ of irreducible polynomials $f \in \mathbb{F}_2[x]$ of degree n with $T_k(f) = t_k$, and $k = 1,\ldots,4$. First we give a formula for the number $F(n,t_1,\ldots,t_4)$ of elements $\beta \in \mathbb{F}_{2^n}$ with $T_k(\beta) = t_k \in \mathbb{F}_2$, for $k = 1,\ldots,4$. Then, we use the idea of Theorem 3.2 in [9] to give the number $N(n,t_1,\ldots,t_4)$ in terms of $F(n,t_1,\ldots,t_4)$. After that, we provide a good approximation of the number $N(n,t_1,\ldots,t_4)$. Finally, for different values of n we present the experimental results related to our approximation.

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

Suppose that $\mathrm{Min}_\beta = f \in \mathbb{F}_2[x]$ of degree n/d is the minimal polynomial of a given $\beta \in \mathbb{F}_{2^n}$. The following lemma regarding the connection between the traces of β and the coefficients of f^d is proved in [2].

Lemma 2.1 *Assume that $f \in \mathbb{F}_2[x]$ of degree n/d is the minimal polynomial of $\beta \in \mathbb{F}_{2^n}$. Then we have $T_k(\beta) = T_k(f^d)$, where $T_k(\beta)$ is the k^{th} trace of β and $T_k(f^d)$ is the k-th trace of f^d, that is, the coefficient of x^{n-k} in f^d, where $k = 1, \dots, n$.*

For a given polynomial $f \in \mathbb{F}_2[x]$ and positive integer $d \geq 1$, the connection between different coefficients of f and f^d is given in the following proposition.

Proposition 2.1 *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) $T_4(f^d) = \binom{d}{4}T_1(f) + \binom{d}{2}T_2(f) + dT_4(f)$.

PROOF. We only prove (*iv*); the proofs of the other parts are similar. Suppose that $f \in \mathbb{F}_2[x]$ is given such that $\deg(f) = n$. We assume that

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0.$$

Therefore, by the multinomial theorem, the polynomial f^d can be given as

$$(f(x))^d = \sum_{k_0+\cdots+k_n=d} \frac{d!(a_{n-1}^{k_1}\cdots a_1^{k_{n-1}}a_0^{k_n})}{k_0!k_1!\dots k_n!}\left(x^{nk_0+(n-1)k_1+\cdots+k_{n-1}}\right).$$

To find $T_4(f^d)$, the coefficient of x^{nd-4} in f^d, we choose $k_0, k_1, \dots, k_{n-1}$ such that $nk_0 + (n-1)k_1 + \cdots + k_{n-1} = nd - 4$. This is possible in one the following three cases:

(1) When $k_0 = d - 4$, $k_1 = 4$ and $k_l = 0$ for all $l \neq 0, 1$; then the corresponding term in f^d is $\binom{d}{4}a_{n-4}x^{nd-4}$, or $\binom{d}{4}T_1(f)x^{nd-4}$.

(2) If $k_0 = d - 2$, $k_2 = 2$ and $k_l = 0$ for any $l \neq 0, 2$; then this gives us the term $\binom{d}{2}a_{n-2}^2x^{nd-4}$ or $\binom{d}{2}T_2(f)x^{nd-4}$ in the polynomial f^d.

(3) When $k_0 = d-1$, $k_4 = 1$ and $k_l = 0$, for $l \neq 0, 4$; we have the term $da_{n-4}x^{nd-4} = dT_4(f)x^{nd-4}$.

From these three cases we have the coefficient of the term x^{nd-4} in the polynomial f^d, which is denoted by $T_4(f^d)$. This proves (iv). ∎

Since the coefficients are in $\mathbb{F}_2$, each of $\binom{d}{1}, \ldots, \binom{d}{4}$ is zero or one. The following proposition gives the different situations, based on $d \equiv i \pmod 8$.

Proposition 2.2 *Let $f \in \mathbb{F}_2[x]$, and $a \equiv b \pmod 8$ be shortened as $a \equiv b$. For any $d \geq 1$ assume that $d \equiv i$, for some $i \in \{0, \ldots, 7\}$. In Table 1 the values of $\binom{d}{1}, \ldots, \binom{d}{4}$ are given. Moreover, for $1 \leq k \leq 4$ Table 1 gives $T_k(f^d)$, that is, the k-th coefficients of f^d in terms of $T_1, \ldots, T_4$ where $T_k = T_k(f)$.*

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

Table 1: Coefficients of f^d, and values of $\binom{d}{1}, \ldots, \binom{d}{4}$.

PROOF. Let $d \geq 1$ be such that $d \equiv 6 \pmod 8$ or $d = 8d' + 6$, for some integer d'. Since d is even, we have

$d \equiv 0 \pmod 8$, $\binom{d}{1} = d \equiv 0 \pmod 8$ and

$$\binom{d}{2} = \frac{d(d-1)}{2} = \frac{(8d'+6)(8d'+5)}{2} = (4d'+3)(8d'+5) \equiv 1,$$

$$\binom{d}{3} = \frac{d(d-1)(d-2)}{6} = (8d'+4)\frac{(8d'+5)(4d'+3)}{3} \equiv 0,$$

$$\binom{d}{4} = \frac{d(d-1)(d-2)(d-3)}{24} = \frac{(4d'+3)(8d'+5)(2d'+1)(8d'+3)}{3} \equiv 1.$$

Hence, by Proposition 2.1 we have $T_1(f^d) = T_3(f^d) = 0$, $T_2(f^d) = T_1(f) = T_1$ and $T_4(f^d) = T_1(f) + T_2(f)$. The proofs for other values of d are similar. ∎

Let us recall that $P(n)$ is the set of all irreducible polynomials of degree n over $\mathbb{F}_2$. We use $c.P(n)$ to denote the multiset that contains c copies of the set $P(n)$. The following lemma gives a formula for the number $F(n,t_1,t_2,t_3,t_4)$.

Lemma 2.2 *Let n be a positive integer and $(t_1,\ldots,t_4) \in \mathbb{F}_2^4$. Assume that $a \equiv b \pmod 8$ is shortened as $a \equiv b$. For any $k = 1,\ldots,4$ and $t_k \in \mathbb{F}_2$, the number of elements $\beta \in \mathbb{F}_{2^n}$ with prescribed traces $T_k(\beta) = t_k$ 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:

$$\begin{aligned}
S_0 &= \{f \in P(n/d) : t_i = 0,\ i = 1,2,3,4\},\\
S_1 &= \{f \in P(n/d) : T_i(f) = t_i,\ i = 1,2,3,4\},\\
S_2 &= \{f \in P(n/d) : t_1 = t_3 = 0,\ T_1(f) = t_2,\ T_2(f) = t_4\},\\
S_3 &= \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_2(f) = t_2,\\
&\qquad T_1(f) + T_3(f) = t_3,\ T_2(f) + T_4(f) = t_4\},\\
S_4 &= \{f \in P(n/d) : t_i = 0,\ i = 1,2,3,\ T_1(f) = t_4\},\\
S_5 &= \{f \in P(n/d) : T_i(f) = t_i,\ i = 1,2,3,\ T_1(f) + T_4(f) = t_4\},\\
S_6 &= \{f \in P(n/d) : t_1 = t_3 = 0,\ T_1(f) = t_2,\ T_1(f) + T_2(f) = t_4\},\\
S_7 &= \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_2(f) = t_2,\\
&\qquad T_1(f) + T_3(f) = t_3,\ T_1(f) + T_2(f) + T_4(f) = t_4\}.
\end{aligned}$$

PROOF. Let $f = \mathrm{Min}_\beta$ be the minimal polynomial of a given $\beta \in \mathbb{F}_{2^n}$. A classic result from finite field theory [8] imply the following equality about multisets:

$$\bigcup_{\beta\in\mathbb{F}_{2^n}} \mathrm{Min}_\beta = \bigcup_{d|n} d.P(d) = \bigcup_{d|n} \frac{n}{d}.P\left(\frac{n}{d}\right).$$

If in the left side of this equality we choose β such that its first four traces be given as $T_k(\beta) = t_k \in \mathbb{F}_2$, where $1 \le k \le 4$, then we get

$$F(n,t_1,t_2,t_3,t_4) = \left| \bigcup_{d|n} \frac{n}{d}.\{f \in P(n/d) : T_k(f^d) = t_k,\ 1 \le k \le 4\} \right|.$$

Then, for different values of d and using Propositions 2.1 and 2.2, we have eight different cases for d, and therefore the number $F(n,t_1,t_2,t_3,t_4)$ can be given by

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

where for $i \in \{0,\ldots,7\}$ the sets S_i are defined as above. ■

3.2 Computing $N(n,t_1,t_2,t_3,t_4)$

To give the formula for the numbers $N(n,t_1,\ldots,t_4)$ in terms of the numbers $F(n,t_1,\ldots,t_4)$, we need the following generalization of Möbius inversion formula that can be obtained from Theorem 3.2 of [9].

Theorem 3 *Assume that $a \equiv b$ denotes $a \equiv b \pmod 8$. Let f_i and g_i be functions defined on $\mathbb{N}$, where $i \in S = \{1,3,5,7\}$. For any $n \in \mathbb{N}$ and $i \in S$ we have*

$$f_i(n)=\sum_{u\in S}\sum_{\substack{d|n \\ d\equiv u}} g_j\left(\frac{n}{d}\right) \quad \textit{if and only if} \quad g_i(n)=\sum_{u\in S}\sum_{\substack{d|n \\ d\equiv u}} \mu(d) f_j\left(\frac{n}{d}\right),$$

where for any $i,u \in S$ we let $j \equiv i\cdot u \pmod 8$.

In the following theorem we give $N(n,t_1,t_2,t_3,t_4)$ in terms of the numbers $F(n,t_1,t_2,t_3,t_4)$. For $t_1,\ldots,t_4 \in \mathbb{F}_2$ there exists 16 cases for (t_1,t_2,t_3,t_4). Since in some of these 16 cases the numbers $N(n,t_1,t_2,t_3,t_4)$ are connected to each other, we divide the 16 cases into 6 different groups.

Theorem 4 *Let $n \geq 4$ be a given integer, and $a \equiv b \pmod 8$ be shortened as $a \equiv b$. Assume $S = \{1,3,5,7\}$, and suppose that the 16 cases of $(t_1,\ldots,t_4) \in \mathbb{F}_2^4$ are divided into 6 different groups $G_1,\ldots,G_6$ which are defined as*

$$\begin{aligned}
G_1 &:= \{(1,1,1,0),(1,1,1,1),(1,0,0,0),(1,0,0,1)\},\\
G_2 &:= \{(0,0,1,0),(0,0,1,1)\},\\
G_3 &:= \{(1,1,0,0),(1,1,0,1),(1,0,1,0),(1,0,1,1)\},\\
G_4 &:= \{(0,1,1,0),(0,1,1,1)\},\\
G_5 &:= \{(0,0,0,0),(0,0,0,1)\},\\
G_6 &:= \{(0,1,0,0),(0,1,0,1)\}.
\end{aligned}$$

Then, the different values of $N(n,t_1,t_2,t_3,t_4)$ are given as follows:

(i) For any $(t_1, t_2, t_3, t_4) \in G_1$ *we have*

$$nN(n, t_1, t_2, t_3, t_4) = \sum_{u \in S} \sum_{\substack{d|n \\ d \equiv u}} \mu(d) F(n/d, t_1', t_2', t_3', t_4'),$$

where $(t_1', t_2', t_3', t_4') \in G_1$*. Moreover, for any* $u \in S$ *each* $(t_1', t_2', t_3', t_4') \in G_1$ *appears exactly once at the right hand side of these four equations.*

(ii) If $(t_1, t_2, t_3, t_4) \in G_2$*, then we have*

$$nN(n, 0, 0, 1, t_4) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) F(n/d, 0, 0, 1, t_4).$$

(iii) If $(t_1, t_2, t_3, t_4) \in G_3$*, then we have*

$$nN(n, t_1, t_2, t_3, t_4) = \sum_{u \in S} \sum_{\substack{d|n \\ d \equiv u}} \mu(d) F(n/d, t_1', t_2', t_3', t_4'),$$

where $(t_1', t_2', t_3', t_4') \in G_3$*, and for a given* $u \in S$*, any of* $(t_1', t_2', t_3', t_4') \in G_3$ *appears exactly once at the right hand side of each of these four equations.*

For $t_4 \in \mathbb{F}_2$ *we define* $\bar{t_4} = 1 + t_4$*. In the following cases, let* $a \equiv b \pmod 4$ *be shortened as* $a \equiv b$*.*

(iv) If $(t_1, t_2, t_3, t_4) \in G_4$*, then* $t_1 = 0$*,* $t_2 = t_3 = 1$ *and in this case we have*

$$nN(n, 0, 1, 1, t_4) = \sum_{\substack{d|n \\ d \equiv 1}} \mu(d) F(n/d, 0, 1, 1, t_4) + \sum_{\substack{d|n \\ d \equiv 3}} \mu(d) F(n/d, 0, 1, 1, \bar{t_4}).$$

(v) For $(t_1, t_2, t_3, t_4) \in G_5$ *we have* $t_1 = t_2 = t_3 = 0$*, and*

$$\begin{aligned} nN(n, 0, 0, 0, t_4) &= \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) F(n/d, 0, 0, 0, t_4) \\ &\quad - [n \text{ even}] \sum_{\substack{d|n,\ \frac{n}{d} \text{ even} \\ d \text{ odd}}} \mu(d) F(n/2d, 0, t_4). \end{aligned}$$

(vi) For any $(t_1, t_2, t_3, t_4) \in G_6$ *we have* $t_1 = t_3 = 0$*,* $t_2 = 1$ *and*

$$\begin{aligned} & nN(n, 0, 1, 0, t_4) \\ = & \sum_{\substack{d|n \\ d \equiv 1}} \mu(d) F(n/d, 0, 1, 0, t_4) - \sum_{\substack{d|n \\ d \equiv 3}} \mu(d) F(n/d, 0, 1, 0, \bar{t_4}) \\ - & [n \text{ even}] \sum_{\substack{d|n \\ \frac{n}{d} \text{ even}}} \mu(d) \left([d \equiv 1] F(n/2d, 1, t_4) - [d \equiv 3] F(n/2d, 1, \bar{t_4}) \right). \end{aligned}$$

PROOF. (i) If we let $(t_1,t_2,t_3,t_4)=(1,1,1,0)$, then by Lemma 2.2 we have

$$
\begin{aligned}
& F(n,1,1,1,0) \\
= & \sum_{\substack{d\mid n \\ d\equiv 1}} \frac{n}{d}\cdot |\{f\in P(n/d): T_i(f)=1,\ i=1,2,3,\ T_4(f)=0\}| \\
& + \sum_{\substack{d\mid n \\ d\equiv 3}} \frac{n}{d}\cdot |\{f\in P(n/d): T_1(f)=T_4(f)=1,\ T_2(f)=T_3(f)=0\}| \\
& + \sum_{\substack{d\mid n \\ d\equiv 5}} \frac{n}{d}\cdot |\{f\in P(n/d): T_i(f)=1,\ i=1,2,3,4\}| \\
& + \sum_{\substack{d\mid n \\ d\equiv 7}} \frac{n}{d}\cdot |\{f\in P(n/d): T_1(f)=1,\ T_i(f)=0,\ i=2,3,4\}| \\
= & \sum_{\substack{d\mid n \\ d\equiv 1}} \frac{n}{d} N(n/d,1,1,1,0) + \sum_{\substack{d\mid n \\ d\equiv 3}} \frac{n}{d} N(n/d,1,0,0,1) \\
& + \sum_{\substack{d\mid n \\ d\equiv 5}} \frac{n}{d} N(n/d,1,1,1,1) + \sum_{\substack{d\mid n \\ d\equiv 7}} \frac{n}{d} N(n/d,1,0,0,0) \\
= & \sum_{u\in S}\sum_{\substack{d\mid n \\ d\equiv u}} \frac{n}{d} N\left(n/d,t_1',t_2',t_3',t_4'\right),
\end{aligned}
$$

such that $(t_1',\dots,t_4')\in G_1=\{(1,1,1,0,),(1,1,1,1),(1,0,0,0),(1,0,0,1)\}$ and $S=\{1,3,5,7\}$. For other $(t_1,t_2,t_3,t_4)\in G_1$ we have

$$
\begin{aligned}
F(n,1,0,0,1) &= \sum_{\substack{d\mid n \\ d\equiv 1}} \frac{n}{d} N(n/d,1,0,0,1) + \sum_{\substack{d\mid n \\ d\equiv 3}} \frac{n}{d} N(n/d,1,1,1,0) \\
&\quad + \sum_{\substack{d\mid n \\ d\equiv 5}} \frac{n}{d} N(n/d,1,0,0,0) + \sum_{\substack{d\mid n \\ d\equiv 7}} \frac{n}{d} N(n/d,1,1,1,1) \\
&= \sum_{u\in S}\sum_{\substack{d\mid n \\ d\equiv u}} \frac{n}{d} N\left(n/d,t_1',t_2',t_3',t_4'\right), \\
F(n,1,1,1,1) &= \sum_{u\in S}\sum_{\substack{d\mid n \\ d\equiv u}} \frac{n}{d} N\left(n/d,t_1',t_2',t_3',t_4'\right), \\
F(n,1,0,0,0) &= \sum_{u\in S}\sum_{\substack{d\mid n \\ d\equiv u}} \frac{n}{d} N\left(n/d,t_1',t_2',t_3',t_4'\right).
\end{aligned}
$$

This implies that for any $(t_1, t_2, t_3, t_4) \in G_1$ we have

$$F(n, t_1, t_2, t_3, t_4) = \sum_{u \in S} \sum_{\substack{d|n \\ d \equiv u}} \frac{n}{d} N\left(n/d, t_1', t_2', t_3', t_4'\right),$$

where $(t_1', t_2', t_3', t_4') \in G_1$. Applying Theorem 3, we obtain the formulas given in (i). For other cases of (t_1, t_2, t_3, t_4) we have similar arguments to find the given formula for the number $N(n, t_1, t_2, t_3, t_4)$. ■

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

In Theorem 4, the formula for the numbers $N(n, t_1, \ldots, t_4)$ is given in terms of the numbers $F(n/d, t_1', \ldots, t_4')$ where $(t_1', \ldots, t_4')$ are from the same groups $G_1, \ldots, G_6$ as (t_1, t_2, t_3, t_4). Unfortunately, it seems hard to find the exact value of $F(n, t_1, t_2, t_3, t_4)$. Hence, we use an estimate for this number to present our approximation for $N(n, t_1, \ldots, t_4)$. In [13], for $n = 2m$, it is conjectured that

$$F(n, t_1, \ldots, t_r) = 2^{n-r} + G(n, t_1, \ldots, t_r) = 2^{n-r} + \sum_{i=0}^{f-1} c_i 2^{m-i}, \qquad (1)$$

for some $1 \leq f \leq m$, and $c_i \in \{-1, 0, 1\}$. Hence, in $F(n, t_1, \ldots, t_r)$ we have a term 2^{n-r} and at most m other powers of two. Our experiments and approximations not only agree with this conjecture but they also allow us to slightly tighten this conjecture, as we will comment later.

From now on, to approximate the number $N(n, t_1, \ldots, t_4)$, we let

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

Using the notation introduced before Theorem 1, we have

$$F(n/d, t_1', \ldots, t_4') \approx \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4}.$$

Since $n \geq 4$, we have $F(n, t_1', \ldots, t_4') \approx 2^{n-4}$.

Assume that $n = 2^{k_0} {p_1}^{k_1} \cdots {p_s}^{k_s} \geq 4$, where $p_1, \ldots, p_s$ are odd prime divisors of n, and $k_0 \geq 0$, $k_1, \ldots, k_s \geq 1$. We use $p_1, \ldots, p_s$ to define the sets $D_1, \ldots, D_s$. Let $D_1 = \{p_1, \ldots, p_s\}$. For any $q = 2, \ldots, s$ we define D_q as the set of all d where $d \mid n$, and d is the product of exactly q distinct primes from D_1. Then, using our previous results, we have the following approximation for $N(n, t_1, \ldots, t_4)$.

Theorem 5 *For any* (t_1, t_2, t_3, t_4) *from groups* $G_1, \ldots, G_4$ *given in Theorem 4, the approximation for the number* $N(n, t_1, t_2, t_3, t_4)$ *can be given as*

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

where the sets $D_1, \ldots, D_s$ *are defined above.*

In group G_5 *the approximation for* $N(n,0,0,0,t_4)$ *is*

$$\begin{aligned} & N(n,0,0,0,t_4) \\ \approx\ & \frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d}\geq 4\right]2^{\frac{n}{d}-4}\right) \\ -\ & [n\ even]\frac{1}{n}\left(F(n/2,0,t_4) + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q F(n/2d,0,t_4)\right). \end{aligned}$$

For $(0,1,0,t_4) \in G_6$*, where* $\bar{t_4} = t_4 + 1$ *for* $t_4 \in \mathbb{F}_2$*, we have*

$$\begin{aligned} & N(n,0,1,0,t_4) \\ \approx\ & \frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d}\geq 4\right]2^{\frac{n}{d}-4} - [n\ even]F(n/2,1,t_4)\right) \\ -\ & [n\ even]\frac{1}{n}\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q[d\equiv 1]F(n/2d,1,t_4) \\ -\ & [n\ even]\frac{1}{n}\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q[d\equiv 3]F(n/2d,1,\bar{t_4}). \end{aligned}$$

PROOF. Let us define $S = \{1,3,5,7\}$, $S' = \{1,3\}$ and $n = 2^{k_0}{p_1}^{k_1}\cdots{p_s}^{k_s}$ be the prime factorization of n. Assume that $D_1, \ldots, D_s$ are defined as earlier. Suppose that $(t_1,t_2,t_3,t_4) = (1,1,1,0) \in \mathrm{G}_1$. Then by Theorem 4 (i) we have

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

The divisor d of n can be 1 or $d \in D_q$, where $q = 1, \dots, s$. Clearly $d = 1$ is in the first sum at the right side, and it defines the term $F(n, 1, 1, 1, 0)$. Then the equation for $N(n, 1, 1, 1, 0)$ can be given as

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

Since $F(n/d, t_1, t_2, t_3, t_4) \approx [\frac{n}{d} \geq 4] 2^{\frac{n}{d}-4}$ and $\mu(d) = (-1)^q$ for all $d \in D_q$, the last equation simplifies to

$$\begin{aligned} & nN(n,1,1,1,0) \\ \approx\; & 2^{n-4} + \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 1}} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} + \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 3}} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \\ + & \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 5}} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} + \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 7}} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \\ =\; & 2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \sum_{u \in S} [d \equiv u]. \end{aligned}$$

For a given $d \in D_q$ where $q = 1, \dots, s$ there exist a *unique* $u \in S = \{1, 3, 5, 7\}$ such that $d \equiv u \pmod 8$, and therefore

$$\sum_{u \in S} [d \equiv u] = 1.$$

This implies that the approximation for $N(n, 1, 1, 1, 0)$ can be given as

$$N(n,1,1,1,0) \approx \frac{1}{n} \left(2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \right).$$

If one follow the same argument, then for any other (t_1, t_2, t_3, t_4) from each of the groups G_1, G_2 and G_3 the same estimate for $N(n, t_1, t_2, t_3, t_4)$ is obtained.

Now let us $(t_1, t_2, t_3, t_4) \in G_4$, and $a \equiv b \pmod 4$ be shortened as $a \equiv b$. Clearly for any $d \in D_q$ where $q = 1, \dots, s$ we have either $d \equiv 1$ or

$d \equiv 3$. Hence, there exists a *unique* $u' \in S' = \{1,3\}$ such that $d \equiv u'$. This implies

$$\sum_{u' \in S'} [d \equiv u'] = 1.$$

If we let $(t_1, t_2, t_3, t_4) = (0,1,1,1)$, then by Theorem 4 (iv) we have

$$\begin{aligned}
& nN(n,0,1,1,1) \\
= \;& F(n,0,1,1,1) + \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 1}} \mu(d) F(n/d,0,1,1,1) \\
+ \;& \sum_{q=1}^{s} \sum_{\substack{d \in D_q \\ d \equiv 3}} \mu(d) F(n/d,0,1,1,0) \\
\approx \;& 2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] \left([d \equiv 1] 2^{\frac{n}{d}-4} + [d \equiv 3] 2^{\frac{n}{d}-4}\right) \\
= \;& 2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \sum_{u' \in S'} [d \equiv u'] \\
= \;& 2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4}.
\end{aligned}$$

This implies that

$$N(n,0,1,1,1) \approx \frac{1}{n} \left(2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} \right).$$

In a similar way, for $(t_1, t_2, t_3, t_4) = (0,1,1,0)$ in group G_4 we have the same estimate for the number $N(n,0,1,0,0)$. This means we have an identical estimate for the number $N(n, t_1, t_2, t_3, t_4)$, when (t_1, t_2, t_3, t_4) is chosen between one of the first 12 cases in groups $G_1, \ldots, G_4$.

In group G_5, let $(t_1, t_2, t_3, t_4) = (0,0,0,0)$. It is clear that any $d \in D_q$ is odd and n/d is even, where $q = 1, \ldots, s$. Then by Theorem 4 (v) we have

$$\begin{aligned}
& nN(n,0,0,0,0) \\
= \;& F(n,0,0,0,0) + \sum_{q=1}^{s} \sum_{d \in S_q} \mu(d) F(n/d,0,0,0,0) \\
- \;& [n \text{ even}] F(n/2,0,0) - [n \text{ even}] \sum_{q=1}^{s} \sum_{d \in D_q} \mu(d) F(n/2d,0,0)
\end{aligned}$$

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

Hence, the approximation for the number $N(n,0,0,0,0)$ can be given as

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

If one follow the same lines, then a similar approximation can be found for the number $N(n,0,0,0,1)$ in G_5. Finally, if $(t_1,t_2,t_3,t_4)=(0,1,0,0)\in G_6$ Theorem 4 (vi) implies that

$$
\begin{aligned}
&nN(n,0,1,0,0)\\
&=\ F(n,0,1,0,0)+\sum_{q=1}^{s}\sum_{\substack{d\in D_q\\ d\equiv 1}}\mu(d)F(n/d,0,1,0,0)\\
&+\ \sum_{q=1}^{s}\sum_{\substack{d\in D_q\\ d\equiv 3}}\mu(d)F(n/d,0,1,0,1)-[n\text{ even}]F(n/2,1,0)\\
&-\ [n\text{ even}]\sum_{q=1}^{s}\sum_{\substack{d\in D_q\\ d\equiv 1}}\mu(d)F(n/2d,1,0)\\
&-\ [n\text{ even}]\sum_{q=1}^{s}\sum_{\substack{d\in D_q\\ d\equiv 3}}\mu(d)F(n/2d,1,1)\\
&\approx\ 2^{n-4}+\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d}\geq 4\right]2^{\frac{n}{d}-4}([d\equiv 1]+[d\equiv 3])\\
&-\ [n\text{ even}]\left(F(n/2,1,0)+\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q[d\equiv 1]F(n/2d,1,0)\right)
\end{aligned}
$$

$$- \quad [n \text{ even}] \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q [d \equiv 3] F(n/2d, 1, 1),$$

which implies that

$$\begin{aligned}
& N(n,0,1,0,0) \\
\approx \quad & \frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q \left[\frac{n}{d} \geq 4\right] 2^{\frac{n}{d}-4} - [n \text{ even}] F(n/2,1,0)\right) \\
- \quad & [n \text{ even}] \frac{1}{n} \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q [d \equiv 1] F(n/2d, 1, 0) \\
- \quad & [n \text{ even}] \frac{1}{n} \sum_{q=1}^{s} \sum_{d \in D_q} (-1)^q [d \equiv 3] F(n/2d, 1, 1).
\end{aligned}$$

A similar proof gives the approximation for $N(n,0,1,0,1)$ in group G_6. ■

From Theorem 5 one can observe that if n is odd, for any $(t_1, t_2, t_3, t_4) \in \mathbb{F}_2^4$ the approximation for $N(n, t_1, t_2, t_3, t_4)$ can be given as

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

3.4 Experimental results

For $n \leq 25$ we use Maple to compute the exact values of $N(n, t_1, \ldots, t_4)$ and our approximations. Due to the lack of space, we report our experimental results for the cases n = 16, 17, 20, 21, 22, 24, 25; see Tables 3, 4, 5, 6, 7, 8 and 9 in the appendix.

For the case $n = 2^{k_0}$ where $k_0 \geq 3$, we have the best approximation. This is true because in this case the only odd divisor of n is $d = 1$. Hence, we have $u = d = 1$. Indeed, for $n = 2^{k_0}$ and $(t_1, \ldots, t_4)$ from groups $G_1, \ldots, G_4$ of Theorem 4, we have

$$nN(n, t_1, t_2, t_3, t_4) = F(n, t_1, t_2, t_3, t_4) \approx 2^{n-4},$$

or $N(n, t_1, \ldots, t_4) \approx 2^{n-4-k_0}$, which is the exact value of $N(n, t_1, \ldots, t_4)$ in most of the first 12 cases in groups G_1, G_2, G_3 and G_4. For the other 4 cases in G_5 and G_6 we have

$$nN(n, t_1, \ldots, t_4) = F(n, t_1, \ldots, t_4) - F(n/2, t_2, t_4) \approx 2^{n-4} - F(n/2, t_2, t_4),$$

which has a small error. For the other values of n, our approximations do not achieve the exact values, but they are very good approximations for the numbers $N(n, t_1, \ldots, t_4)$.

To compare our estimate and the exact value of $N(n, t_1, \ldots, t_4)$ in each table we let

$$\text{error} = \text{exact}(N(n, t_1, \ldots, t_4)) - \text{estimate}(N(n, t_1, \ldots, t_4)).$$

Then for different case number $i = 1, \ldots, 16$ we define

$$\rho_i = \begin{cases} \frac{\text{estimate of } N}{\text{exact } N} & \text{if error is positive,} \\ \frac{\text{exact } N}{\text{estimate of } N} & \text{if error is negative,} \\ 1 & \text{if error is zero.} \end{cases}$$

Now assume that $\rho = \min\{\rho_1, \ldots, \rho_{16}\}$. Therefore $\rho \leq 1$, and if $\rho = 1$ then our estimate is the exact value of $N(n, t_1, \ldots, t_4)$. For degree $n = 16, 20, 22, 24$ we have $\rho = 0.9504, 0.9884, 0.9916, 0.9971$, while for $n = 17, 21, 25$ we have $\rho = 0.9712$, 0.9968, 0.9978. Numerical results give evidence that as n grows, ρ gets closer to one, which means for large n our approximation for $N(n, t_1, \ldots, t_4)$ is likely to be closer to its exact value. One can see this from Theorem 5. For even n, in the first 12 cases of Theorem 5 which are given as groups $G_1, \ldots, G_4$ we have

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

In the double-sum we divide n by d, and for a large n the term $2^{\frac{n}{d}-4}$ has a smaller weight comparing with 2^{n-4}. This is also true for the remaining four cases given in groups G_5 and G_6.

We conclude this section with two remarks. In our approximations for odd n, there are no extra terms, and simply in all the 16 cases for $(t_1, \ldots, t_4)$ we have the same approximation given by Equation (2). Moreover, we observe that as n grows, the total number of irreducible polynomials with given $(t_1, \ldots, t_4)$ and the total number of irreducible polynomials given by our approximations are very close.

4 Approximating $N(n, t_1, \ldots, t_r)$, for $r \geq 5$

Let us consider $r \geq 5$. We give a formula for $N(n, t_1, \ldots, t_r)$ in terms of $F(n, t_1, \ldots, t_r)$. First we state the formula for $N(n, t_1, \ldots, t_5)$. Then we present our approximation for $N(n, t_1, \ldots, t_r)$, where $r = 5, 6, 7$. Finally, for $r \geq 8$ we explain the methodology to find the formula for $N(n, t_1, \ldots, t_r)$.

4.1 Approximating $N(n, t_1, \ldots, t_r)$, where $r = 5, 6$ and 7

In Section 3 to study the number $N(n, t_1, \ldots, t_4)$, we found a formula for $F(n, t_1, \ldots, t_4)$ in terms of the sets $S_0, \ldots, S_7$; see Lemma 2.2. Each of these sets are defined based on the connections between the coefficients of the polynomials f and f^d given in Propositions 2.1 and 2.1, where $f \in \mathbb{F}_2[x]$ such that $\deg(f) = n$ and $d \geq 1$. In general, for any $j \geq 1$,

$$T_j(f^d) = \sum_{k|j} \binom{d}{k} T_{j/k}(f). \tag{3}$$

Let us fix $5 \leq r \leq 7$. Then by (3), and for any $1 \leq j \leq r$, the j-th coefficient of f^d depends on $\binom{d}{k}$, for some $k \in \{1, \ldots, 7\}$. Similar to Proposition 2.2, for different $i = 0, \ldots, 7$ if $d \equiv i \pmod 8$, one can show that $\binom{d}{1}, \ldots, \binom{d}{7}$ are zero or one. The values of $\binom{d}{1}, \ldots, \binom{d}{7}$ are given in Table 2. To find our

$d \equiv i$	$\binom{d}{1}$	$\binom{d}{2}$	$\binom{d}{3}$	$\binom{d}{4}$	$\binom{d}{5}$	$\binom{d}{6}$	$\binom{d}{7}$
$d \equiv 0$	0	0	0	0	0	0	0
$d \equiv 1$	1	0	0	0	0	0	0
$d \equiv 2$	0	1	0	0	0	0	0
$d \equiv 3$	1	1	1	0	0	0	0
$d \equiv 4$	0	0	0	1	0	0	0
$d \equiv 5$	1	0	0	1	1	0	0
$d \equiv 6$	0	1	0	1	0	1	0
$d \equiv 7$	1	1	1	1	1	1	1

Table 2: Values of $\binom{d}{1}, \ldots, \binom{d}{7}$, for integer $d \geq 1$.

formula for $F(n, t_1, \ldots, t_r)$ where $5 \leq r \leq 7$, we make slight changes in the definition of the sets $S_0, \ldots, S_7$ given in Lemma 2.2. The following lemma gives the numbers $F(n, t_1, \ldots, t_5)$. We omit its proof since it is similar to the proof of Lemma 2.2.

Lemma 5.1 *For a given integer $n \geq 5$, we have*

$$F(n, t_1, \ldots, t_5) = \sum_{i=0}^{7} \bigcup_{\substack{d|n \\ d \equiv i}} \frac{n}{d} \cdot |S_i|,$$

where $a \equiv b$ represents $a \equiv b \pmod 8$, and the sets $S_0, \ldots, S_7$ are defined as:

$$S_0 = \{f \in P(n/d) : t_i = 0,\ i = 1, \ldots, 5\},$$
$$S_1 = \{f \in P(n/d) : T_i(f) = t_i,\ i = 1, \ldots, 5\},$$

$S_2 = \{f \in P(n/d) : t_1 = t_3 = t_5 = 0,\ T_1(f) = t_2,\ T_2(f) = t_4\},$
$S_3 = \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_i(f) = t_i,\ i = 2, 3,$
$\quad T_2(f) + T_4(f) = t_4,\ T_5(f) = t_5\},$
$S_4 = \{f \in P(n/d) : t_i = 0,\ i = 1, 2, 3, 5,\ T_1(f) = t_4\},$
$S_5 = \{f \in P(n/d) : T_i(f) = t_i,\ i = 1, 2, 3,\ T_1(f) + T_i(f) = t_i,\ i = 4, 5\},$
$S_6 = \{f \in P(n/d) : t_1 = t_3 = t_5 = 0,\ T_1(f) = t_2,\ T_1(f) + T_2(f) = t_4\},$
$S_7 = \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_i(f) = t_i,\ i = 2, 3, 5,$
$\quad T_1(f) + T_2(f) + T_4(f) = t_4\}.$

Lemma 5.1 and Theorem 3 immediately give the following theorem for $N(n, t_1, \ldots, t_5)$.

Theorem 6 *Let $n \geq 5$ be a given integer and suppose that $a \equiv b$ denotes $a \equiv b \pmod 8$. Assume that $S = \{1, 3, 5, 7\}$, and for any $(t_1, \ldots, t_5) \in \mathbb{F}_2^5$ let $(t_1, \ldots, t_4)$ be from one of the 6 groups $G_1, \ldots, G_6$ defined in Theorem 4. For different $(t_1, \ldots, t_4)$ the formulas for $N(n, t_1, \ldots, t_5)$ are given as follows.*

(i) If $(t_1, \ldots, t_4) \in G_1$, then

$$nN(n, t_1, \ldots, t_5) = \sum_{u \in S} \sum_{\substack{d|n \\ d \equiv u}} \mu(d) F(n/d, t_1', \ldots, t_5'),$$

where $(t_1', \ldots, t_4') \in G_1$, and for any $u \in S$ each $(t_1', \ldots, t_5')$ appears exactly once at the right hand side of these 8 equations.

(ii) If $(t_1, \ldots, t_4) \in G_2$, then $t_1 = t_2 = 0$, $t_3 = 1$ and

$$nN(n, 0, 0, 1, t_4, t_5) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) F(n/d, 0, 0, 1, t_4, t_5).$$

(iii) If $(t_1, \ldots, t_4) \in G_3$, then

$$nN(n, t_1, \ldots, t_5) = \sum_{u \in S} \sum_{\substack{d|n \\ d \equiv u}} \mu(d) F(n/d, t_1', \ldots, t_5'),$$

where $(t_1', \ldots, t_4') \in G_3$, and for a given $u \in S$ any of $(t_1', \ldots, t_5')$ appears exactly once at the right hand side of these 8 equations.

In the following cases, let $a \equiv b \pmod 4$ be shortened as $a \equiv b$, and for $t_4 \in \mathbb{F}_2$ let $\bar{t_4} = 1 + t_4$.

(iv) *If* $(t_1,\ldots,t_4)\in G_4$, *then* $t_1=0,\ t_2=t_3=1$ *and*

$$\begin{aligned} & nN(n,0,1,1,t_4,t_5) \\ = & \sum_{\substack{d|n \\ d\equiv 1}}\mu(d)F(n/d,0,1,1,t_4,t_5)+\sum_{\substack{d|n \\ d\equiv 3}}\mu(d)F(n/d,0,1,1,\bar{t_4},t_5). \end{aligned}$$

(v) *For* $(t_1,\ldots,t_4)\in G_5$ *we have* $t_1=t_2=t_3=0$, *and*

$$\begin{aligned} & nN(n,0,0,0,t_4,t_5) \\ = & \sum_{\substack{d|n \\ d \text{ odd}}}\mu(d)F(n/d,0,0,0,t_4,t_5) \\ - & [n \text{ even}]\sum_{\substack{d|n,\ \frac{n}{d} \text{ even} \\ d \text{ odd}}}\mu(d)F(n/2d,0,t_4). \end{aligned}$$

(vi) *For any* $(t_1,\ldots,t_4)\in G_6$ *we have* $t_1=t_3=0,\ t_2=1$ *and*

$$\begin{aligned} & nN(n,0,1,0,t_4,t_5) \\ = & \sum_{\substack{d|n \\ d\equiv 1}}\mu(d)F(n/d,0,1,0,t_4,t_5)+\sum_{\substack{d|n \\ d\equiv 3}}\mu(d)F(n/d,0,1,0,\bar{t_4},t_5) \\ - & [n \text{ even}]\sum_{\substack{d|n,\ \frac{n}{d} \text{ even} \\ d\equiv 1}}\mu(d)F(n/2d,1,t_4) \\ - & [n \text{ even}]\sum_{\substack{d|n,\ \frac{n}{d} \text{ even} \\ d\equiv 3}}\mu(d)F(n/2d,1,\bar{t_4}). \end{aligned}$$

For $i=1,\ldots,6$ one can obtain $(t_1,\ldots,t_5)$ in group G_i of Theorem 6 by adding two cases of $t_5=0,1$ to the corresponding $(t_1,\ldots,t_4)$ in group G_i from Theorem 4. One can easily obtain the formulas for the numbers $N(n,t_1,\ldots,t_r)$ when $r=6,7$, using a similar process like the one used to obtain Theorem 6.

With an argument similar to Theorem 5, we have the following approximation for $N(n,t_1,\ldots,t_r)$ where $r=5,6,7$.

Theorem 7 *Let* $n=2^{k_0}p_1{}^{k_1}\cdots p_s{}^{k_s}$, *where* $p_1,\ldots,p_s$ *are odd prime divisors of* n, *and* $k_0\geq 0$, $k_1,\ldots,k_s\geq 1$. *Let* $D_1,\ldots,D_q$ *be the same sets defined before Theorem 5. For any* $(t_1,\ldots,t_r)\in\mathbb{F}_2^r$ *where* $r=5,6,7$ *we consider* $(t_1,\ldots,t_4)$ *in one of the 6 groups* $G_1,\ldots,G_6$ *given in Theorem 4.*

If n *is an even integer, then we have the following cases.*

(i) For $(t_1, \ldots, t_4)$ from $G_1, \ldots, G_4$ the approximation for $N(n, t_1, \ldots, t_r)$ can be given as

$$N(n, t_1, \ldots, t_r) \approx \frac{1}{n}\left(2^{n-r} + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d} \geq r\right]2^{\frac{n}{d}-r}\right).$$

(ii) For any $(t_1, \ldots, t_4) \in G_5$ we have

$$\begin{aligned} N(n, t_1, \ldots, t_r) \approx\ & \frac{1}{n}(2^{n-r} - F(n/2, t_2, t_4)) \\ & + \frac{1}{n}\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left(\left[\frac{n}{d} \geq r\right]2^{\frac{n}{d}-r} - F(n/2d, t_2, t_4)\right). \end{aligned}$$

(iii) If $(t_1, \ldots, t_4) \in G_6$, then we have

$$\begin{aligned} & N(n, t_1, \ldots, t_r) \\ \approx\ & \frac{1}{n}\left(2^{n-r} - F(n/2, t_2, t_4) + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d} \geq r\right]2^{\frac{n}{d}-r}\right) \\ -\ & \frac{1}{n}\sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q([d \equiv 1]F(n/2d, t_2, t_4) + [d \equiv 3]F(n/2d, t_2, \bar{t_4})), \end{aligned}$$

where $\bar{t_4} = t_4 + 1$, for $t_4 \in \mathbb{F}_2$.

If n is an odd integer, then for any $(t_1, \ldots, t_r) \in \mathbb{F}_2^r$ we have

$$N(n, t_1, \ldots, t_r) \approx \frac{1}{n}\left(2^{n-r} + \sum_{q=1}^{s}\sum_{d\in D_q}(-1)^q\left[\frac{n}{d} \geq r\right]2^{\frac{n}{d}-r}\right).$$

As examples of our approximations, see Tables 10 and 11 in the appendix where we give the computational results for $N(n, t_1, \ldots, t_5)$ when $n = 16, 18$.

4.2 Approximating $N(n, t_1, \ldots, t_r)$, where $r \geq 8$

Now we are ready to explain how to derive a formula for $N(n, t_1, \ldots, t_r)$, $r \geq 8$, and its approximation.

In the general r case, to study the number $N(n, t_1, \ldots, t_r)$, we let r be in the range $[2^q, 2^{q+1} - 1]$, where $q \geq 2$. For $f \in \mathbb{F}_2[x]$, $d \geq 1$ and

$1 \leq j \leq r$, Equation (3) gives the coefficients of f^d in terms of the coefficients of f and $\binom{d}{1}, \binom{d}{2} \ldots, \binom{d}{2^{q+1}-1}$. For each $k = 1, \ldots, 2^{q+1} - 1$ the number $\binom{d}{k}$ is either zero or one, depending on $d \equiv i \pmod{2^{q+1}}$ where $i = 0, \ldots, 2^{q+1} - 1$. Then, similar to Lemma 2.2, to give the formula for $F(n, t_1, \ldots, t_r)$ we need 2^{q+1} sets S_i where $i = 0, \ldots, 2^{q+1} - 1$. Moreover, in the definition of each set S_i, the congruence is mod 2^{q+1}. Suppose that $S = \{1, 3, \ldots, 2^{q+1} - 1\}$. Then using Theorem 3.2 of [9] we can give a formula, similar to the one in Theorem 3, to find the number $N(n, t_1, \ldots, t_r)$ in terms of the numbers $F(n, t_1, \ldots, t_r)$ as we did in Theorem 4. Finally, let $(t_1, \ldots, t_4)$ be from different groups $G_1, \ldots, G_6$ as defined in Theorem 4. By expanding each $(t_1, \ldots, t_4)$ to $(t_1, \ldots, t_r)$, as we did in the case $r = 5$, we have the new groups $G_1, \ldots, G_6$. This implies that any $(t_1, \ldots, t_r) \in \mathbb{F}_2^r$ can be from one of the new groups $G_1, \ldots, G_6$, and the formula for the number $N(n, t_1, \ldots, t_r)$, similar to Theorem 5, can be given when $(t_1, \ldots, t_r)$ is from different groups $G_1, \ldots, G_6$. We show a concrete example. Let $r = 8$ and $n = 22$; Table 12 in the appendix gives the values of $N(22, t_1, \ldots, t_8)$ where $(t_1, \ldots, t_8) \in G_1$. This accounts for 64 cases of the $2^8 = 256$ cases when $r = 8$. Due to the lack of space we omit the rest of the table.

5 Conclusion

We study the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_2$ where the coefficients of the terms $x^{n-1}, \ldots, x^{n-r}$ are prescribed. For $r \geq 4$ finding the exact values of $N(n, t_1, \ldots, t_r)$ seems involved and difficult. We give an approximation for these numbers using an estimate for the number $F(n, t_1, \ldots, t_r)$ of elements $\beta \in \mathbb{F}_{2^n}$ with given traces $T_i(\beta) = t_i$ and $i = 1, \ldots, r$.

If $n = 2m$, then by Equation (1) it is conjectured that in $F(n, t_1, \ldots, t_r)$ we have 2^{n-r}, and at most m other powers of two. If n is odd, we let $n = 2m + 1$ and we assume Equation (1) for the number $F(n, t_1, \ldots, t_r)$. Our experimental results show that for any even or odd n, there exists a small number of these powers in $F(n, t_1, \ldots, t_r)$ which is much smaller than m. This means that most of the coefficients c_i in Equation (1) are zero, and our approximation for $N(n, t_1, \ldots, t_r)$ is likely to be very close to its exact value.

The *exact* estimation of the number of irreducible polynomials over $\mathbb{F}_2$ with several prescribed coefficients remains an open problem for future research. We hope that the results proved in this paper help in solving this problem.

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] 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.)

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

[9] C. R. Miers and F. Ruskey, Counting strings with given elementary symmetric function evaluations II: circular strings, *SIAM J. Discrete Mathematics*, **18** (2004), 71-82.

[10] B. Omidi Koma, D. Panario and Q. Wang, The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms, *Discrete Mathematics*, **310** (2010), 1282-1292.

[11] B. Omidi Koma, *The Number of Irreducible Polynomials Over a Finite Field With Prescribed Coefficients*, PhD. Thesis, (2010), 87-117.

[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.

Appendix

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	256	260	4	0.9846
2	$(1,0,0,1)$	256	260	4	0.9846
3	$(1,1,1,1)$	256	252	-4	0.9843
4	$(1,0,0,0)$	256	252	-4	0.9843
5	$(0,0,1,0)$	256	256	0	1
6	$(0,0,1,1)$	256	256	0	1
7	$(1,1,0,0)$	256	256	0	1
8	$(1,0,1,1)$	256	256	0	1
9	$(1,1,0,1)$	256	256	0	1
10	$(1,0,1,0)$	256	256	0	1
11	$(0,1,1,1)$	256	264	8	0.9697
12	$(0,1,1,0)$	256	264	8	0.9697
13	$(0,0,0,0)$	252.5	240	-12.5	0.9504
14	$(0,0,0,1)$	251.5	256	-4.5	0.9824
15	$(0,1,0,0)$	252	248	-4	0.9841
16	$(0,1,0,1)$	252	248	-4	0.9841
Total		4080	4080		

Table 3: Different values of $N(16, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	481.88	492	10.1	0.9795
2	$(1,0,0,1)$	481.88	484	2.1	0.9957
3	$(1,1,1,1)$	481.88	468	-13.9	0.9712
4	$(1,0,0,0)$	481.88	491	9.1	0.9815
5	$(0,0,1,0)$	481.88	468	-13.9	0.9712
6	$(0,0,1,1)$	481.88	492	10.1	0.9795
7	$(1,1,0,0)$	481.88	476	-5.9	0.9878
8	$(1,0,1,1)$	481.88	492	10.1	0.9795
9	$(1,1,0,1)$	481.88	484	2.1	0.9957
10	$(1,0,1,0)$	481.88	468	-13.9	0.9712
11	$(0,1,1,1)$	481.88	476	-5.9	0.9878
12	$(0,1,1,0)$	481.88	484	2.1	0.9957
13	$(0,0,0,0)$	481.88	491	9.1	0.9815
14	$(0,0,0,1)$	481.88	484	2.1	0.9957
15	$(0,1,0,0)$	481.88	468	-13.9	0.9712
16	$(0,1,0,1)$	481.88	492	10.1	0.9795
Total		7710.4	7710		

Table 4: Different values of $N(17, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	3276.75	3275	-1.75	0.9995
2	$(1,0,0,1)$	3276.75	3304	27.25	0.9917
3	$(1,1,1,1)$	3276.75	3304	27.25	0.9917
4	$(1,0,0,0)$	3276.75	3275	-1.75	0.9995
5	$(0,0,1,0)$	3276.75	3264	-12.75	0.9961
6	$(0,0,1,1)$	3276.75	3315	38.25	0.9884
7	$(1,1,0,0)$	3276.75	3264	-12.75	0.9961
8	$(1,0,1,1)$	3276.75	3264	-12.75	0.9961
9	$(1,1,0,1)$	3276.75	3264	-12.75	0.9961
10	$(1,0,1,0)$	3276.75	3264	-12.75	0.9961
11	$(0,1,1,1)$	3276.75	3264	-12.75	0.9961
12	$(0,1,1,0)$	3276.75	3264	-12.75	0.9961
13	$(0,0,0,0)$	3264	3264	0	1
14	$(0,0,0,1)$	3264	3264	0	1
15	$(0,1,0,0)$	3264.75	3280	15.25	0.9953
16	$(0,1,0,1)$	3263.25	3248	-15.25	0.9953
Total		53350	52377		

Table 5: Different values of $N(20, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	6241.14	6221	-20.86	0.9968
2	$(1,0,0,1)$	6241.14	6224	-17.86	0.9973
3	$(1,1,1,1)$	6241.14	6237	-3.86	0.9993
4	$(1,0,0,0)$	6241.14	6258	17.14	0.9973
5	$(0,0,1,0)$	6241.14	6221	-20.86	0.9968
6	$(0,0,1,1)$	6241.14	6237	-3.86	0.9993
7	$(1,1,0,0)$	6241.14	6258	17.14	0.9973
8	$(1,0,1,1)$	6241.14	6221	-20.86	0.9968
9	$(1,1,0,1)$	6241.14	6237	-3.86	0.9993
10	$(1,0,1,0)$	6241.14	6237	-3.86	0.9993
11	$(0,1,1,1)$	6241.14	6237	-3.86	0.9993
12	$(0,1,1,0)$	6241.14	6258	17.14	0.9973
13	$(0,0,0,0)$	6241.14	6224	-17.86	0.9973
14	$(0,0,0,1)$	6241.14	6258	17.14	0.9973
15	$(0,1,0,0)$	6241.14	6221	-20.86	0.9968
16	$(0,1,0,1)$	6241.14	6237	-3.86	0.9993
Total		99858.24	99858		

Table 6: Different values of $N(21, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	11915.64	11904	-11.64	0.999
2	$(1,0,0,1)$	11915.64	11904	-11.64	0.999
3	$(1,1,1,1)$	11915.64	11904	-11.64	0.999
4	$(1,0,0,0)$	11915.64	11904	-11.64	0.999
5	$(0,0,1,0)$	11915.64	11992	76.36	0.9936
6	$(0,0,1,1)$	11915.64	11816	-99.64	0.9916
7	$(1,1,0,0)$	11915.64	11904	-11.64	0.999
8	$(1,0,1,1)$	11915.64	11952	36.36	0.9969
9	$(1,1,0,1)$	11915.64	11904	-11.64	0.999
10	$(1,0,1,0)$	11915.64	11949	33.36	0.9972
11	$(0,1,1,1)$	11915.64	11816	-99.64	0.9916
12	$(0,1,1,0)$	11915.64	11992	76.36	0.9936
13	$(0,0,0,0)$	11893.14	11928	34.86	0.997
14	$(0,0,0,1)$	11891.68	11880	-11.68	0.999
15	$(0,1,0,0)$	11891.73	11880	-11.73	0.999
16	$(0,1,0,1)$	11893.09	11928	34.91	0.997
Total		190557.32	190557		

Table 7: Different values of $N(22, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	43690	43759	69	0.9984
2	$(1,0,0,1)$	43690	43759	69	0.9984
3	$(1,1,1,1)$	43690	43621	-69	0.9984
4	$(1,0,0,0)$	43690	43621	-69	0.9984
5	$(0,0,1,0)$	43690	43754	64	0.9985
6	$(0,0,1,1)$	43690	43754	64	0.9985
7	$(1,1,0,0)$	43690	43690	0	1
8	$(1,0,1,1)$	43690	43690	0	1
9	$(1,1,0,1)$	43690	43690	0	1
10	$(1,0,1,0)$	43690	43690	0	1
11	$(0,1,1,1)$	43690	43711	21	0.9995
12	$(0,1,1,0)$	43690	43711	21	0.9995
13	$(0,0,0,0)$	43646.25	43520	-126.25	0.9971
14	$(0,0,0,1)$	43648.75	43562	-86.75	0.9980
15	$(0,1,0,0)$	43647.5	43669	21.5	0.9995
16	$(0,1,0,1)$	43647.5	43669	21.5	0.9995
Total		698870	698870		

Table 8: Different values of $N(24, t_1, t_2, t_3, t_4)$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	exact value	error	ρ_i
1	$(1,1,1,0)$	83886	83920	34	0.9996
2	$(1,0,0,1)$	83886	83824	-62	0.9997
3	$(1,1,1,1)$	83886	83811	-75	0.9991
4	$(1,0,0,0)$	83886	84071	185	0.9978
5	$(0,0,1,0)$	83886	83811	-75	0.9991
6	$(0,0,1,1)$	83886	83920	34	0.9996
7	$(1,1,0,0)$	83886	83907	21	0.9997
8	$(1,0,1,1)$	83886	83920	34	0.9996
9	$(1,1,0,1)$	83886	83824	-62	0.9997
10	$(1,0,1,0)$	83886	83811	-75	0.9991
11	$(0,1,1,1)$	83886	83907	21	0.9997
12	$(0,1,1,0)$	83886	83920	34	0.9996
13	$(0,0,0,0)$	83886	84071	185	0.9978
14	$(0,0,0,1)$	83886	83824	-62	0.9997
15	$(0,1,0,0)$	83886	83811	-75	0.9991
16	$(0,1,0,1)$	83886	83920	34	0.9996
Total		1342176	1342176		

Table 9: Different values of $N(25, t_1, t_2, t_3, t_4)$.

Case No.	$(t_1,\ldots,t_5)$	our estimate	exact value	error	ρ_i
1	$(1,1,1,0,0)$	128	128	0	1
2	$(1,0,0,0,0)$	128	128	0	1
3	$(1,1,1,1,0)$	128	124	-4	0.9688
4	$(1,0,0,1,0)$	128	132	4	0.9697
5	$(1,1,1,0,1)$	128	132	4	0.9697
6	$(1,0,0,0,1)$	128	124	-4	0.9688
7	$(1,1,1,1,1)$	128	128	0	1
8	$(1,0,0,1,1)$	128	128	0	1
9	$(0,0,1,0,0)$	128	120	-8	0.9375
10	$(0,0,1,0,1)$	128	136	8	0.9412
11	$(0,0,1,1,0)$	128	120	-8	0.9375
12	$(0,0,1,1,1)$	128	136	8	0.9412
13	$(1,1,0,1,1)$	128	128	0	1
14	$(1,1,0,0,1)$	128	128	0	1
15	$(1,0,1,1,1)$	128	128	0	1
16	$(1,0,1,0,1)$	128	128	0	1
17	$(1,1,0,0,0)$	128	128	0	1
18	$(1,0,1,0,0)$	128	128	0	1
19	$(1,1,0,1,0)$	128	128	0	1
20	$(1,0,1,1,0)$	128	128	0	1
21	$(0,1,1,0,0)$	128	136	8	0.9412
22	$(0,1,1,0,1)$	128	128	0	1
23	$(0,1,1,1,0)$	128	136	8	0.9412
24	$(0,1,1,1,1)$	128	128	0	1
25	$(0,0,0,0,0)$	124.5	120	-4.5	0.9639
26	$(0,0,0,0,1)$	123.5	120	-3.5	0.9717
27	$(0,0,0,1,0)$	124	120	-4	0.9677
28	$(0,0,0,1,1)$	124	136	8	0.9118
29	$(0,1,0,0,0)$	124	120	-4	0.9677
30	$(0,1,0,0,1)$	124	128	4	0.9688
31	$(0,1,0,1,0)$	124	120	-4	0.9677
32	$(0,1,0,1,1)$	124	128	4	0.9688
Total		4064	4080		

Table 10: Different values of $N(16, t_1, \ldots, t_5)$.

Case No.	$(t_1, \ldots, t_5)$	our estimate	exact value	error	ρ_i
1	$(1,1,1,0,0)$	455	469	14	0.9701
2	$(1,0,0,0,0)$	455	448	-11	0.9846
3	$(1,1,1,1,0)$	455	448	-11	0.9846
4	$(1,0,0,1,0)$	455	448	-11	0.9846
5	$(1,1,1,0,1)$	455	448	-11	0.9846
6	$(1,0,0,0,1)$	455	448	-11	0.9846
7	$(1,1,1,1,1)$	455	469	14	0.9701
8	$(1,0,0,1,1)$	455	448	-11	0.9846
9	$(0,0,1,0,0)$	455	462	7	0.9848
10	$(0,0,1,0,1)$	455	452	-3	0.9934
11	$(0,0,1,1,0)$	455	448	-7	0.9846
12	$(0,0,1,1,1)$	455	444	-11	0.9846
13	$(1,1,0,1,1)$	455	445	-10	0.9780
14	$(1,1,0,0,1)$	455	448	-7	0.9846
15	$(1,0,1,1,1)$	455	469	14	09701
16	$(1,0,1,0,1)$	455	448	-7	0.9846
17	$(1,1,0,0,0)$	455	479	24	0.9499
18	$(1,0,1,0,0)$	455	469	14	0.9701
19	$(1,1,0,1,0)$	455	448	-7	0.9846
20	$(1,0,1,1,0)$	455	448	-7	0.9846
21	$(0,1,1,0,0)$	455	444	-11	0.9846
22	$(0,1,1,0,1)$	455	448	-11	0.9846
23	$(0,1,1,1,0)$	455	452	-3	0.9934
24	$(0,1,1,1,1)$	455	469	14	0.9701
25	$(0,0,0,0,0)$	447	444	-3	0.9933
26	$(0,0,0,0,1)$	447	469	22	0.9531
27	$(0,0,0,1,0)$	448	452	4	0.9912
28	$(0,0,0,1,1)$	448	448	0	1
29	$(0,1,0,0,0)$	448	444	-4	0.9911
30	$(0,1,0,0,1)$	448	469	21	0.952
31	$(0,1,0,1,0)$	448	452	4	09912
32	$(0,1,0,1,1)$	448	448	0	1
Total		14502	14532		

Table 11: Different values of $N(18, t_1, \ldots, t_5)$.

Case No.	$(t_1, \ldots, t_8)$	our estimate	exact value	error	ρ_i
1	(1, 1, 1, 0, 0, 0, 0, 0)	744.73	732	-12.73	0.9829
2	(1, 1, 1, 0, 0, 0, 0, 1)	744.73	716	-28.73	0.9614
3	(1, 1, 1, 0, 0, 0, 1, 0)	744.73	756	11.27	0.9851
4	(1, 1, 1, 0, 0, 0, 1, 1)	744.73	756	11.27	0.9851
5	(1, 1, 1, 0, 0, 1, 0, 0)	744.73	762	17.27	0.9773
6	(1, 1, 1, 0, 0, 1, 0, 1)	744.73	758	13.27	0.9825
7	(1, 1, 1, 0, 0, 1, 1, 0)	744.73	733	11.73	0.9842
8	(1, 1, 1, 0, 0, 1, 1, 1)	744.73	736	8.73	0.9883
9	(1, 1, 1, 0, 1, 0, 0, 0)	744.73	741	3.73	0.9950
10	(1, 1, 1, 0, 1, 0, 0, 1)	744.73	751	6.27	0.9917
11	(1, 1, 1, 0, 1, 0, 1, 0)	744.73	761	16.27	0.9786
12	(1, 1, 1, 0, 1, 0, 1, 1)	744.73	723	21.73	0.9708
13	(1, 1, 1, 0, 1, 1, 0, 0)	744.73	741	3.73	0.9950
14	(1, 1, 1, 0, 1, 1, 0, 1)	744.73	751	6.27	0.9917
15	(1, 1, 1, 0, 1, 1, 1, 0)	744.73	723	21.73	0.9708
16	(1, 1, 1, 0, 1, 1, 1, 1)	744.73	761	16.27	0.9786
17	(1, 0, 0, 1, 0, 0, 0, 0)	744.73	741	3.73	0.9950
18	(1, 0, 0, 1, 0, 0, 0, 1)	744.73	729	15.73	0.9789
19	(1, 0, 0, 1, 0, 0, 1, 0)	744.73	771	26.27	0.9659
20	(1, 0, 0, 1, 0, 0, 1, 1)	744.73	745	0.27	0.9996
21	(1, 0, 0, 1, 0, 1, 0, 0)	744.73	721	-23.73	0.9682
22	(1, 0, 0, 1, 0, 1, 0, 1)	744.73	731	-13.73	0.9816
23	(1, 0, 0, 1, 0, 1, 1, 0)	744.73	743	-1.73	0.9977
24	(1, 0, 0, 1, 0, 1, 1, 1)	744.73	765	20.27	0.9735
25	(1, 0, 0, 1, 1, 0, 0, 0)	744.73	728	-16.73	0.9775
26	(1, 0, 0, 1, 1, 0, 0, 1)	744.73	744	-0.23	0.999
27	(1, 0, 0, 1, 1, 0, 1, 0)	744.73	740	-4.73	0.9936
28	(1, 0, 0, 1, 1, 0, 1, 1)	744.73	740	-4.73	0.9936
29	(1, 0, 0, 1, 1, 1, 0, 0)	744.73	764	19.27	0.9748
30	(1, 0, 0, 1, 1, 1, 0, 1)	744.73	748	3.27	0.9956
31	(1, 0, 0, 1, 1, 1, 1, 0)	744.73	748	3.27	0.9956
32	(1, 0, 0, 1, 1, 1, 1, 1)	744.73	744	-0.23	0.999
33	(1, 1, 1, 1, 0, 0, 0, 0)	744.73	745	0.27	0.9996
34	(1, 1, 1, 1, 0, 0, 0, 1)	744.73	747	2.27	0.9970
35	(1, 1, 1, 1, 0, 0, 1, 0)	744.73	769	24.27	0.9684
36	(1, 1, 1, 1, 0, 0, 1, 1)	744.73	715	-29.73	0.9601
37	(1, 1, 1, 1, 0, 1, 0, 0)	744.73	745	0.27	0.9996
38	(1, 1, 1, 1, 0, 1, 0, 1)	744.73	747	2.27	0.9970
39	(1, 1, 1, 1, 0, 1, 1, 0)	744.73	715	-29.73	0.9601
40	(1, 1, 1, 1, 0, 1, 1, 1)	744.73	769	24.27	0.9684
41	(1, 1, 1, 1, 1, 0, 0, 0)	744.73	760	15.27	0.9799
42	(1, 1, 1, 1, 1, 0, 0, 1)	744.73	760	15.27	0.9799
43	(1, 1, 1, 1, 1, 0, 1, 0)	744.73	736	8.73	0.9883
44	(1, 1, 1, 1, 1, 0, 1, 1)	744.73	736	8.73	0.9883
45	(1, 1, 1, 1, 1, 1, 0, 0)	744.73	718	-26.73	0.9641
46	(1, 1, 1, 1, 1, 1, 0, 1)	744.73	762	17.27	0.9773
47	(1, 1, 1, 1, 1, 1, 1, 0)	744.73	740	-4.73	0.9936
48	(1, 1, 1, 1, 1, 1, 1, 1)	744.73	740	-4.73	0.9936
49	(1, 0, 0, 0, 0, 0, 0, 0)	744.73	728	-16.73	0.9775
50	(1, 0, 0, 0, 0, 0, 0, 1)	744.73	744	-0.23	0.999
51	(1, 0, 0, 0, 0, 0, 1, 0)	744.73	740	-4.73	0.9936
52	(1, 0, 0, 0, 0, 0, 1, 1)	744.73	740	-4.73	0.9936
53	(1, 0, 0, 0, 0, 1, 0, 0)	744.73	764	19.27	0.9748
54	(1, 0, 0, 0, 0, 1, 0, 1)	744.73	748	3.27	0.9956
55	(1, 0, 0, 0, 0, 1, 1, 0)	744.73	744	-0.23	0.999
56	(1, 0, 0, 0, 0, 1, 1, 1)	744.73	744	-0.23	0.999
57	(1, 0, 0, 0, 1, 0, 0, 0)	744.73	721	-23.73	0.9682
58	(1, 0, 0, 0, 1, 0, 0, 1)	744.73	733	11.73	0.9842
59	(1, 0, 0, 0, 1, 0, 1, 0)	744.73	765	20.27	0.9735
60	(1, 0, 0, 0, 1, 0, 1, 1)	744.73	743	-1.73	0.9977
61	(1, 0, 0, 0, 1, 1, 0, 0)	744.73	747	2.27	0.9970
62	(1, 0, 0, 0, 1, 1, 0, 1)	744.73	729	15.73	0.9789
63	(1, 0, 0, 0, 1, 1, 1, 0)	744.73	745	0.27	0.9996
64	(1, 0, 0, 0, 1, 1, 1, 1)	744.73	771	26.27	0.9659
Total		47662.72	47616		

Table 12: Values of $N(22, t_1, \ldots, t_8)$, for different $(t_1, \ldots, t_8) \in G_1$.