The Number of Irreducible Polynomials over GF(2) with Given Trace and Subtrace

K. Cattell[*] C.R. Miers[†] F. Ruskey[‡] J. Sawada[§]
M. Serra[¶]

Abstract

The *trace* of a degree n polynomial $p(x)$ over GF(2) is the coefficient of x^{n-1} and the *subtrace* is the coefficient of x^{n-2}. We derive an explicit formula for the number of irreducible degree n polynomials over GF(2) that have a given trace and subtrace. The trace and subtrace of an element $\beta \in GF(2^n)$ are defined to be the coefficients of x^{n-1} and x^{n-2}, respectively, in the polynomial $q(x) = \prod_{i=0}^{n-1}(x + \beta^{2^i})$. We also derive an explicit formula for the number of elements of $GF(2^n)$ of given trace and subtrace. Moreover, a new two equation Möbius-type inversion formula is proved.

Keywords: Irreducible polynomial, minimal polynomial, trace, subtrace, Möbius inversion.

[*] Hewlett-Packard Labs, Santa Rosa, California. e-mail: kevin_cattell@hp.com

[†] Dept. of Mathematics, University of Victoria, Canada. Research supported in part by NSERC. e-mail: crmiers@math.uvic.ca

[‡] Dept. of Computer Science, University of Victoria, Canada Research supported in part by NSERC. e-mail: fruskey@csr.uvic.ca

[§] Dept. of Computer Science, University of Victoria, Canada research supported in part by NSERC. e-mail: jsawada@csr.uvic.ca

[¶] Dept. of Computer Science, University of Victoria, Canada research supported in part by NSERC. e-mail: mserra@csr.uvic.ca

1 Introduction

The *trace* of a degree n polynomial $p(x)$ over GF(2) is the coefficient of x^{n-1} and the *subtrace* is the coefficient of x^{n-2}. It is well known that the formula

$$L(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d} \tag{1}$$

counts the number of degree n irreducible polynomials over $GF(2)$, where $\mu(d)$ is the Möbius function. Less well-known is the formula

$$L_1(n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d} \tag{2}$$

which counts the number of degree n irreducible polynomials over GF(2) that have trace 1. This result is later proved in Theorem 3. The purpose of this paper is to refine these formulas by enumerating the irreducible degree n polynomials over GF(2) with given trace and subtrace. This enumeration uses numbers familiar to those working on the combinatorics of words. In order to state our main result we need to develop some notation.

The *cotrace* of $p(x)$ is the coefficient of x^1. The *reciprocal* of $p(x)$ is the polynomial $p^*(x) := x^n p(1/x)$. A polynomial is *self-reciprocal* if it is equal to its reciprocal.

An aperiodic word of length n has n distinct circular shifts, exactly one of which is minimal in the lexicographic order. Such a word is called a *Lyndon word.* If $L(n,k)$ is the number of length n Lyndon words containing exactly k 1's, it is known that

$$L(n,k) = \frac{1}{n} \sum_{d \mid \gcd(n,k)} \mu(d) \binom{n/d}{k/d}. \tag{3}$$

A simple proof may be found in [2].

For $S \subseteq \{0,1,\ldots,n\}$, let

$$e(S) = \sum_{k \in S} L(n,k).$$

It can be readily seen that $e(\{0,1,\ldots,n\}) = L(n)$ and $e(\{k \mid k \text{ is odd }\}) = L_1(n)$, the number of irreducible polynomials with trace 1. Our main result comes from the correspondence in enumeration between Lyndon words and irreducible polynomials. The main theorem says that the number of degree

n irreducible polynomials with given trace and subtrace is obtained by taking every fourth entry from the n-th row of the table of $L(n, k)$ numbers.

MAIN THEOREM. *The number of irreducible polynomials of degree n over $GF(2)$ with given trace and subtrace is covered by one of the following cases:*

- *The number of trace 0, subtrace 1 polynomials is* $e(\{k \mid (k+n) \equiv 0 \pmod 4\})$.
- *The number of trace 1, subtrace 0 polynomials is* $e(\{k \mid (k+n) \equiv 1 \pmod 4\})$.
- *The number of trace 0, subtrace 0 polynomials is* $e(\{k \mid (k+n) \equiv 2 \pmod 4\})$.
- *The number of trace 1, subtrace 1 polynomials is* $e(\{k \mid (k+n) \equiv 3 \pmod 4\})$.

Subsequent to our discovery of this theorem in 1998, we learned in 2001 that it had been anticipated in a more general form by Kuz'min [8]. However, the approach and proofs in the two papers are disjoint. Whereas [8] makes extensive use of the theory of L-functions and character theory for groups, our proofs are combinatorial in nature and elementary in that they rely only on the intrinsic (vector space) structure of the field. We feel that the novelty of our approach justifies publication. Furthermore, we have recently learned that Yucas and Mullen [12] have used the machinery and approach developed in this paper to count the number of polynomials over GF(2) with given trace, subtrace, and sub-subtrace.

The organization of this paper is as follows. We begin in Section 2 by proving a novel two-equation Möbius inversion formula. In Section 3, we derive the formula (2) for $L_1(n)$, first as a corollary of known results, and then using a method which is indicative of our approach for the more refined formulas for trace and subtrace. In Section 4, we prove a series of technical results which are then used to count the elements in $GF(2^n)$ with given trace and subtrace. In Section 5, we prove the main theorem.

Congruences modulo 4 are crucial and pervasive in this paper and expressions of the form $x \equiv y \pmod 4$ are shortened to read $x \equiv y$. We use Jungnickel [6] as a reference for terminology and basic results from finite field theory.

2 A generalized Möbius inversion formula

The approach we follow in this section is similar to that found in Knuth, Graham, and Patashnik [7]. The defining property of the Möbius function is

$$\sum_{d|n} \mu(d) = \llbracket n = 1 \rrbracket, \tag{4}$$

where $\llbracket P \rrbracket$ for proposition P represents the "Iversonian convention": $\llbracket P \rrbracket$ has value 1 if P is true and value 0 if P is false (see [7], pg. 24).

LEMMA 1

$$\sum_{\substack{k|n \\ k\equiv 1}} \sum_{\substack{l|(n/k) \\ l\equiv 1}} a_{k,kl} = \sum_{\substack{m|n \\ m\equiv 1}} \sum_{\substack{k|m \\ k\equiv 1}} a_{k,m} \tag{5}$$

$$\sum_{\substack{k|n \\ k\equiv 3}} \sum_{\substack{l|(n/k) \\ l\equiv 1}} a_{k,kl} = \sum_{\substack{m|n \\ m\equiv 3}} \sum_{\substack{k|m \\ k\equiv 3}} a_{k,m} \tag{6}$$

$$\sum_{\substack{k|n \\ k\equiv 1}} \sum_{\substack{l|(n/k) \\ l\equiv 3}} a_{k,kl} = \sum_{\substack{m|n \\ m\equiv 3}} \sum_{\substack{k|m \\ k\equiv 1}} a_{k,m} \tag{7}$$

$$\sum_{\substack{k|n \\ k\equiv 3}} \sum_{\substack{l|(n/k) \\ l\equiv 3}} a_{k,kl} = \sum_{\substack{m|n \\ m\equiv 1}} \sum_{\substack{k|m \\ k\equiv 3}} a_{k,m} \tag{8}$$

We will prove one of these (8); the proofs of the others are similar. First observe that if $m = kl$, then

$$\llbracket l \equiv 3 \rrbracket \llbracket k \equiv 3 \rrbracket = \llbracket kl \equiv 1 \rrbracket \llbracket k \equiv 3 \rrbracket = \llbracket m \equiv 1 \rrbracket \llbracket k \equiv 3 \rrbracket.$$

We now rewrite the left side of (8),

$$\begin{aligned} \sum_{\substack{k|n \\ k\equiv 3}} \sum_{\substack{l|(n/k) \\ l\equiv 3}} a_{k,kl} &= \sum_{j,m} \sum_{k,l>0} a_{k,kl} \llbracket n = jk \rrbracket \llbracket n/k = ml \rrbracket \llbracket k \equiv 3 \rrbracket \llbracket l \equiv 3 \rrbracket \\ &= \sum_{m} \sum_{k,l>0} a_{k,kl} \llbracket n = mkl \rrbracket \llbracket k \equiv 3 \rrbracket \llbracket l \equiv 3 \rrbracket, \end{aligned}$$

and the right side of (8)

$$\begin{aligned}\sum_{\substack{m|n\\m\equiv 1}}\sum_{\substack{k|m\\k\equiv 3}} a_{k,m} &= \sum_{j,l}\sum_{k,m>0} a_{k,m}[\![n=jm]\!][\![m=kl]\!][\![m\equiv 1]\!][\![k\equiv 3]\!]\\ &= \sum_{m}\sum_{k,l>0} a_{k,kl}[\![n=mkl]\!][\![k\equiv 3]\!][\![l\equiv 3]\!],\end{aligned}$$

and observe that they are identical. □

THEOREM 1 *Suppose that $A(n)$, $B(n)$, $\alpha(n)$, and $\beta(n)$ are functions on numbers. Then*

$$A(n)=\sum_{\substack{d|n\\d\equiv 1}}\alpha(\frac{n}{d})+\sum_{\substack{d|n\\d\equiv 3}}\beta(\frac{n}{d}) \quad \text{and}$$

$$B(n)=\sum_{\substack{d|n\\d\equiv 1}}\beta(\frac{n}{d})+\sum_{\substack{d|n\\d\equiv 3}}\alpha(\frac{n}{d})$$

if and only if

$$\alpha(n)=\sum_{\substack{d|n\\d\equiv 1}}\mu(d)A(\frac{n}{d})+\sum_{\substack{d|n\\d\equiv 3}}\mu(d)B(\frac{n}{d}) \quad \text{and}$$

$$\beta(n)=\sum_{\substack{d|n\\d\equiv 1}}\mu(d)B(\frac{n}{d})+\sum_{\substack{d|n\\d\equiv 3}}\mu(d)A(\frac{n}{d}).$$

Proof Consider the sum:

$$f(n)=\sum_{\substack{d|n\\d\equiv 1}}\alpha(\frac{n}{d})+\sum_{\substack{d|n\\d\equiv 3}}\beta(\frac{n}{d}).$$

Plugging in the expressions for α and β we obtain (applying (4) and Lemma 1)

$$\begin{aligned}
f(n) &= \sum_{\substack{d|n\\ d\equiv 1}} \left[\sum_{\substack{c|(n/d)\\ c\equiv 1}} \mu(c)A(\frac{n/d}{c}) + \sum_{\substack{c|(n/d)\\ c\equiv 3}} \mu(c)B(\frac{n/d}{c}) \right] + \\
&\quad \sum_{\substack{d|n\\ d\equiv 3}} \left[\sum_{\substack{c|(n/d)\\ c\equiv 1}} \mu(c)B(\frac{n/d}{c}) + \sum_{\substack{c|(n/d)\\ c\equiv 3}} \mu(c)A(\frac{n/d}{c}) \right] \\
&= \sum_{\substack{d|n\\ d\equiv 1}} \sum_{\substack{c|(n/d)\\ c\equiv 1}} \mu(c)A(\frac{n/d}{c}) + \sum_{\substack{d|n\\ d\equiv 1}} \sum_{\substack{c|(n/d)\\ c\equiv 3}} \mu(c)B(\frac{n/d}{c}) + \\
&\quad \sum_{\substack{d|n\\ d\equiv 3}} \sum_{\substack{c|(n/d)\\ c\equiv 1}} \mu(c)B(\frac{n/d}{c}) + \sum_{\substack{d|n\\ d\equiv 3}} \sum_{\substack{c|(n/d)\\ c\equiv 3}} \mu(c)A(\frac{n/d}{c}) \\
&= \sum_{\substack{m|n\\ m\equiv 1}} \sum_{\substack{d|m\\ d\equiv 1}} \mu(\frac{m}{d})A(\frac{n}{m}) + \sum_{\substack{m|n\\ m\equiv 3}} \sum_{\substack{d|m\\ d\equiv 1}} \mu(\frac{m}{d})B(\frac{n}{m}) + \\
&\quad \sum_{\substack{m|n\\ m\equiv 3}} \sum_{\substack{d|m\\ d\equiv 3}} \mu(\frac{m}{d})B(\frac{n}{m}) + \sum_{\substack{m|n\\ m\equiv 1}} \sum_{\substack{d|m\\ d\equiv 3}} \mu(\frac{m}{d})A(\frac{n}{m}) \\
&= \sum_{\substack{m|n\\ m\equiv 1}} A(\frac{n}{m}) \sum_{\substack{d|m\\ d\equiv 1}} \mu(\frac{m}{d}) + \sum_{\substack{m|n\\ m\equiv 3}} B(\frac{n}{m}) \sum_{\substack{d|m\\ d\equiv 1}} \mu(\frac{m}{d}) + \\
&\quad \sum_{\substack{m|n\\ m\equiv 3}} B(\frac{n}{m}) \sum_{\substack{d|m\\ d\equiv 3}} \mu(\frac{m}{d}) + \sum_{\substack{m|n\\ m\equiv 1}} A(\frac{n}{m}) \sum_{\substack{d|m\\ d\equiv 3}} \mu(\frac{m}{d}) \\
&= \sum_{\substack{m|n\\ m\equiv 1}} A(\frac{n}{m}) \sum_{\substack{d|m\\ d \text{ odd}}} \mu(\frac{m}{d}) + \sum_{\substack{m|n\\ m\equiv 3}} B(\frac{n}{m}) \sum_{\substack{d|m\\ d \text{ odd}}} \mu(\frac{m}{d}) \\
&= \sum_{\substack{m|n\\ m\equiv 1}} A(\frac{n}{m}) \sum_{d|m} \mu(d) + \sum_{\substack{m|n\\ m\equiv 3}} B(\frac{n}{m}) \sum_{d|m} \mu(d) \\
&= A(n)
\end{aligned}$$

Verification in the other direction is similar and is omitted. □

Setting $\alpha(n) = \beta(n)$ (or $A(n) = B(n)$) gives us the following corollary.

COROLLARY 1 *Suppose that $A(n)$ and $\alpha(n)$ are functions on numbers. Then*

$$A(n) = \sum_{\substack{d|n\\ d \text{ odd}}} \alpha(\frac{n}{d}) \quad \textit{if and only if} \quad \alpha(n) = \sum_{\substack{d|n\\ d \text{ odd}}} \mu(d)A(\frac{n}{d}).$$

3 Counting trace 1 irreducible polynomials

In this section we count the trace 1 irreducible polynomials. We begin by introducing some notation that will be used in the remainder of the paper.

If q is the power of a prime, $F = GF(q)$, $E = GF(q^n)$, and $\beta \in E$, we define

$$Tr_{E/F}(\beta) := \sum_{k=0}^{n-1} \beta^{q^k}.$$

In the case $q = p$ where p a prime, one writes $Tr_E(\beta)$ instead of $Tr_{E/F}(\beta)$. The quantity $Tr_E(\beta)$ is called the *absolute trace* of β and is the negative of the coefficient of x^{n-1} in $f(x) = \prod_{i=0}^{n-1}(x - \beta^{p^i})$. We also write $Tr(f)$ instead of $Tr_E(\beta)$.

In this paper we deal only with the case $p = 2$ and adopt the following notation. If $E = GF(2^n)$ and $\beta \in E$, $Tr(\beta) := Tr_E(\beta)$. If $F = GF(2^m)$, $E = GF(2^n)$, with $F \subseteq E$ and $\beta \in E$, $Tr_{2^n:2^m}(\beta) := Tr_{E/F}(\beta)$. If $\alpha \in GF(2^m) \subseteq GF(2^n)$, $Tr_{2^m}(\alpha) := Tr_F(\alpha)$. If $\beta \in GF(2^n)$, $St(\beta)$ is the coefficient of x^{n-2} in $f(x) = \prod_{i=0}^{n-1}(x + \beta^{2^i})$. We also write $St(f)$ instead of $St(\beta)$.

For polynomial f of degree n over GF(2), define

$$f^Q(x) := x^n f(x + x^{-1}).$$

The following three results are all stated and proved in the book of Jungnickel [6].

LEMMA 2 ([6], PG. 77) *Let g be any monic self-reciprocal polynomial of degree $2n$ over GF(2). Then there exists a polynomial f of degree n over GF(2) such that $g = f^Q$. If g is irreducible, then f is also irreducible.*

THEOREM 2 ([6], PG. 77) *The number of monic self-reciprocal irreducible polynomials of degree $2n$ over GF(2) is $L_1(n)$.*

LEMMA 3 ([6], PG. 80) *Let $f(x)$ be degree n irreducible polynomial over GF(2). Then f^Q is irreducible if and only the cotrace of f is 1.*

We now show that the number of degree n irreducible polynomials of trace 1 equals $L_1(n)$ using two methods. The first proof uses the previous results, while the second proof is illustrative of the approach to be used in proving the main theorem.

THEOREM 3 *The number of degree n irreducible polynomials over GF(2) with trace 1 is $L_1(n)$.*

First Proof. We count the number of irreducible degree n polynomials over GF(2) with cotrace 1; this is the same as the number with trace 1 since the map $f \to f^*$ is a bijection and sends the irreducible polynomials to irreducible polynomials.

Let f be such a polynomial. By Lemma 3, f^Q is irreducible. Clearly f^Q is self-reciprocal and has degree $2n$. On the other hand, if g is a self-reciprocal irreducible polynomial of degree $2n$, then by Lemma 2 there is an irreducible polynomial f of degree n such that $g = f^Q$. By Lemma 3 the cotrace of f is 1. Hence there is a one-to-one correspondence between self-reciprocal irreducible polynomials of degree $2n$ and irreducible polynomials of degree n with cotrace 1. Thus, by Theorem 2, the number of irreducible polynomials of degree n with cotrace 1 is $L_1(n)$. □

We now give an alternative proof for the result above, emphasizing different aspects.

Second Proof. If $\beta \in GF(2^n)$ and $p(x)$ is the minimal polynomial of β, denoted $Min(\beta)$, then

$$p(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{2^{d-1}}),$$

where $d \mid n$.

Let $\mathbf{Irr}(n)$ denote the set of all irreducible polynomials over GF(2) of degree n. By $a \cdot \mathbf{Irr}(n)$ we denote the multiset consisting of a copies of $\mathbf{Irr}(n)$. Classic results of finite field theory imply the following equality of multisets:

$$\bigcup_{\beta \in \mathrm{GF}(2^n)} Min(\beta) = \bigcup_{d|n} d \cdot \mathbf{Irr}(d) = \bigcup_{d|n} \frac{n}{d} \cdot \mathbf{Irr}(\frac{n}{d}). \qquad (9)$$

From (9) it is easy to derive (1) via a standard application of Möbius inversion.

Now we restrict the equality (9) to trace 1 field elements to obtain:

$$\begin{aligned} \bigcup_{\substack{\beta\in GF(2^n)\\ Tr(\beta)=1}} Min(\beta) &= \bigcup_{d|n} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p^d)=1\} && (10)\\ &= \bigcup_{d|n} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \ : \ d\cdot Tr(p)=1\} && (11)\\ &= \bigcup_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p)=1\}. && (12)\end{aligned}$$

The set of trace 0 and trace 1 elements partitions $GF(2^n)$ into two sets of equal size (since trace is additive and $\alpha \to \alpha+1$ is a bijection). Hence, the number of trace 1 elements in $GF(2^n)$ is 2^{n-1}. Thus if we take cardinalities in (12), we obtain:

$$2^{n-1} = \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} Irr(\frac{n}{d},1), \qquad (13)$$

where $Irr(n,1)$ denotes the number of irreducible polynomials of degree n and trace 1. The fact that $Irr(n,1) = L_1(n)$ now follows by Corollary 1. □

4 Counting elements in $GF(2^n)$ of given trace and subtrace

In this section we count the elements in GF(2^n) with given trace and subtrace. We first prove two technical lemmata.

LEMMA 4 *Suppose $\beta \in$ GF(2^n) with minimal polynomial p of degree n/d. Then $Tr(\beta)$ is the coefficient of x^{n-1} in p^d and $St(\beta)$ is the coefficient of x^{n-2} in p^d.*

Proof We consider only the subtrace. The proof for the trace is almost identical.

The subtrace of β is the coefficient of x^{n-2} in

$$q(x) = \prod_{i=0}^{n-1}(x+\beta^{2^i}).$$

Since p has degree n/d, the degree of β must be n/d; i.e., $\beta^{2^{i+n/d}} = \beta^{2^i}$. Therefore,

$$q(x) = (\prod_{i=0}^{n/d}(x + \beta^{2^{i-1}}))^d = p^d.$$

$\square$

Let $L_0(k)$ be the number of irreducible polynomials of degree k with trace 0.

LEMMA 5

$$\sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_1(\frac{n}{d}) = \sum_{\substack{d|n \\ d\equiv 0}} \frac{n}{d} L(\frac{n}{d}) + \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_0(\frac{n}{d}) = \begin{cases} 2^{n/2-1} & \textit{if } n \textit{ even} \\ 0 & \textit{if } n \textit{ odd} \end{cases}$$

Proof: Let

$$A(n) = \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_1(\frac{n}{d}),$$

$$B(n) = \sum_{\substack{d|n \\ d\equiv 0}} \frac{n}{d} L(\frac{n}{d}) + \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_0(\frac{n}{d}).$$

If n odd then clearly there are no even divisors of n. But in each of the expressions $A(n)$ and $B(n)$ the divisors of n must be even. Thus if n is odd then both $A(n)$ and $B(n)$ must be 0.

Consider n even. We first prove that $A(n) = 2^{n/2-1}$ and then use this result to prove $B(n) = 2^{n/2-1}$.

$$\begin{aligned} A(n) &= \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_1(\frac{n}{d}) \\ &= \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} (\frac{d}{2n} \sum_{\substack{k|\frac{n}{d} \\ k \text{ odd}}} \mu(k) 2^{n/dk}) \\ &= \frac{1}{2} \sum_{\substack{d|n \\ d\equiv 2}} \sum_{\substack{dk|n \\ k \text{ odd}}} \mu(k) 2^{n/dk} \\ &= \frac{1}{2} \sum_{\substack{dk|n \\ d\equiv 2 \\ k \text{ odd}}} \mu(k) 2^{n/dk}. \end{aligned}$$

We now let $m = dk$ and substitute for d:

$$\begin{aligned} A(n) &= \frac{1}{2} \sum_{\substack{m\mid n \\ \frac{m}{k}\equiv 2 \\ k \text{ odd}}} \mu(k) 2^{n/m} \\ &= \frac{1}{2} \sum_{\substack{m\mid n \\ m\equiv 2 \\ k\mid \frac{m}{2}}} \mu(k) 2^{n/m} \\ &= \frac{1}{2} \sum_{\substack{m\mid n \\ m\equiv 2}} 2^{n/m} \sum_{k\mid \frac{m}{2}} \mu(k) \\ &= \frac{1}{2} \sum_{\substack{m\mid n \\ m\equiv 2}} 2^{n/m} [\![m = 2]\!] \\ &= 2^{n/2-1}. \end{aligned}$$

We now consider $B(n) + A(n)$ for n even.

$$\begin{aligned} B(n) + A(n) &= \sum_{\substack{d\mid n \\ d\equiv 0}} \frac{n}{d} L(\frac{n}{d}) + \sum_{\substack{d\mid n \\ d\equiv 2}} \frac{n}{d} L_0(\frac{n}{d}) + \sum_{\substack{d\mid n \\ d\equiv 2}} \frac{n}{d} L_1(\frac{n}{d}) \\ &= \sum_{\substack{d\mid n \\ d\equiv 0}} \frac{n}{d} L(\frac{n}{d}) + \sum_{\substack{d\mid n \\ d\equiv 2}} \frac{n}{d} L(\frac{n}{d}) \\ &= \sum_{\substack{d\mid n \\ d \text{ even}}} \frac{n}{d} L(\frac{n}{d}) \\ &= \sum_{d\mid \frac{n}{2}} \frac{n}{2d} L(\frac{n}{2d}) \\ &= 2^{n/2}. \end{aligned}$$

Thus since $A(n) = 2^{n/2-1}$ for n even, by performing simple subtraction we get the result $B(n) = 2^{n/2-1}$ for n even. □

We first modify (12) to add a restriction on the subtrace, and then express the result as a disjoint union depending on the value of d mod 4.

$$\begin{aligned}
\bigcup_{\substack{\beta\in \mathrm{GF}(2^n)\\ Tr(\beta)=t\\ St(\beta)=s}} Min(\beta) &= \bigcup_{d|n} \frac{n}{d}\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; Tr(p^d)=t \text{ and } St(p^d)=s\} \\
&= \bigcup_{d|n} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; d\cdot Tr(p)=t,\; d\cdot St(p)+ \\
&\quad \binom{d}{2} Tr(p)=s\} \qquad (14) \\
&= \bigcup_{\substack{d|n\\ d\equiv 0}} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; t=0, s=0\}\cup \\
&\quad \bigcup_{\substack{d|n\\ d\equiv 1}} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; Tr(p)=t,\; St(p)=s\}\cup \\
&\quad \bigcup_{\substack{d|n\\ d\equiv 2}} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; t=0,\; Tr(p)=s\}\cup \\
&\quad \bigcup_{\substack{d|n\\ d\equiv 3}} \frac{n}{d}\cdot\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; Tr(p)=t,\; St(p)=s+t\}.
\end{aligned}$$

Taking cardinalities, we obtain an expression for $F(n,t,s)$, the number of elements of $\mathrm{GF}(2^n)$ of trace t and subtrace s.

$$\begin{aligned}
F(n,t,s) &\overset{\mathrm{def}}{\equiv} \sum_{\substack{\beta\in \mathrm{GF}(2^n)\\ Tr(\beta)=t\\ St(\beta)=s}} |Min(\beta)| \\
&= \sum_{\substack{d|n\\ d\equiv 0}} \frac{n}{d}\cdot|\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; t=0, s=0\}|+ \\
&\quad \sum_{\substack{d|n\\ d\equiv 1}} \frac{n}{d}\cdot|\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; Tr(p)=t,\; St(p)=s\}|+ \\
&\quad \sum_{\substack{d|n\\ d\equiv 2}} \frac{n}{d}\cdot|\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; t=0,\; Tr(p)=s\}|+ \\
&\quad \sum_{\substack{d|n\\ d\equiv 3}} \frac{n}{d}\cdot|\{p\in \mathbf{Irr}(\frac{n}{d}) \;:\; Tr(p)=t,\; St(p)=s+t\}|.
\end{aligned}$$

We use the notation $P(n,t,s) = |\{p\in \mathbf{Irr}(n) : Tr(p)=t, St(p)=s\}|$. If $t=1$ and $s=0$ then we obtain

$$\begin{aligned} F(n,1,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot |\{p \in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p) = 1, St(p) = 0\}| + \\ & \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot |\{p \in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p) = 1, St(p) = 1\}| \\ &= \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot P(n/d,1,0) + \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot P(n/d,1,1). \end{aligned} \tag{15}$$

If $t = s = 1$ then we obtain

$$\begin{aligned} F(n,1,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot |\{p \in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p) = 1, St(p) = 1\}| + \\ & \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot |\{p \in \mathbf{Irr}(\frac{n}{d}) \ : \ Tr(p) = 1, St(p) = 0\}| \\ &= \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot P(n/d,1,1) + \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot P(n/d,1,0). \end{aligned} \tag{16}$$

If $t = s = 0$ then we obtain

$$\begin{aligned} F(n,0,0) &= \sum_{\substack{d|n \\ d\equiv 0}} \frac{n}{d} L(\frac{n}{d}) + \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_0(\frac{n}{d}) + \\ & \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot P(n/d,0,0) + \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot P(n/d,0,0) \\ &= [\![n \text{ even}]\!] \ 2^{n/2-1} + \sum_{\substack{d|n \\ d \text{ odd}}} \frac{n}{d} \cdot P(n/d,0,0). \end{aligned} \tag{17}$$

If $t = 0$ and $s = 1$ then we obtain

$$\begin{aligned} F(n,0,1) &= \sum_{\substack{d|n \\ d\equiv 2}} \frac{n}{d} L_1(\frac{n}{d}) + \\ & \sum_{\substack{d|n \\ d\equiv 1}} \frac{n}{d} \cdot P(n/d,0,1) + \sum_{\substack{d|n \\ d\equiv 3}} \frac{n}{d} \cdot P(n/d,0,1) \\ &= [\![n \text{ even}]\!]\ 2^{n/2-1} + \sum_{\substack{d|n \\ d \text{ odd}}} \frac{n}{d} \cdot P(n/d,0,1). \qquad (18) \end{aligned}$$

The justification for equations (17) and (18) is from Lemma 5.

Before proceeding further we need to determine the values of $F(n,t,s)$.

Recall that $F(n,t,s)$ denotes the number of elements $\beta \in GF(2^n)$ for which $Tr(\beta) = t$ and $St(\beta) = s$. Our purpose in this section is to prove the following theorem, which gives an explicit formula for the number of elements of given trace and subtrace over $GF(2^n)$.

Define $S_r(n)$ to be the sum

$$S_r(n) := \sum_{i\equiv r} \binom{n}{i}.$$

THEOREM 4

$$F(n,t,s) = \begin{cases} S_{t+2\bar{s}}(n) & \textit{if } n \textit{ even} \\ S_{t+2s}(n) & \textit{if } n \textit{ odd.} \end{cases}$$

The proof is divided into 3 cases, Case 1: n odd, Case 2: $n \equiv 2$, and Case 3: $n \equiv 0$. There is one subsection per case. The first two cases use the existence of a self-dual normal basis. A self-dual normal basis exists for GF(2^n) if and only if n is not a multiple of 4. When $4|n$ there is no self-dual normal basis and the derivation is considerably more complex. Before we consider the three cases, we need to prove four technical lemmata.

A ***basis*** for $GF(2^n)$ is a set of n linearly independent elements of $GF(2^n)$. A basis is a ***normal basis*** if it is of the form $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$. If $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ is a normal basis, then it is ***self-dual*** if $Tr(\alpha^{2^i}\alpha^{2^j}) = [\![i = j]\!]$.

The numbers $S_r(n)$ can also be expressed as the sum of two powers of 2. The $T[n,r]$ values mentioned in Lemma 6 are from Table 1.

	$r \equiv 0$	$r \equiv 1$	$r \equiv 2$	$r \equiv 3$
$n \equiv 0$	$+$	0	$-$	0
$n \equiv 1$	$+$	$+$	$-$	$-$
$n \equiv 2$	0	$+$	0	$-$
$n \equiv 3$	$-$	$+$	$+$	$-$
$n \equiv 4$	$-$	0	$+$	0
$n \equiv 5$	$-$	$-$	$+$	$+$
$n \equiv 6$	0	$-$	0	$+$
$n \equiv 7$	$+$	$-$	$-$	$+$

Table 1: $T[n,r]$

LEMMA 6

$$S_r(n) = 2^{n-2} + \begin{cases} +2^{\lfloor n/2 \rfloor - 1} & \textit{if } T[n,r] = + \\ -2^{\lfloor n/2 \rfloor - 1} & \textit{if } T[n,r] = - \\ 0 & \textit{if } T[n,r] = 0. \end{cases}$$

Proof This lemma may be proved by induction on n using Table 1 and the Pascal triangle recurrence relation (indexing done mod 4):

$$S_r(n) = S_r(n-1) + S_{r-1}(n-1)$$

□

We now prove a combinatorial lemma that will be of use in the first two subsections.

LEMMA 7 *With summation done mod 2,*

$$|\{a_0 a_1 \cdots a_{n-1} \in \{0,1\}^n : \sum_{0 \le i < n} a_i = t, \sum_{0 \le i < j < n} a_i a_j = s\}| = S_{t+2s}(n).$$

Proof We prove this lemma by focusing on the number of 1's in the binary string $a_0 a_1 \cdots a_{n-1}$. Suppose that the string has k ones. Clearly, $t \equiv k \bmod 2$.

Notice that the expression $\sum_{0 \le i < j < n} a_i a_j$ is simply counting the number of ways to pair up two distinct 1's in the string where order does not matter.

Thus $\sum_{0\le i<j<n} a_i a_j = \binom{k}{2}$. Since $\binom{k}{2} = k(k-1)/2$, we deduce that $\binom{k}{2}$ mod $2 = 0$ if and only if either k or $k-1$ is congruent to 0 mod 4. This means that k must be congruent to 0 or 1 mod 4 if $s = 0$. Since the above condition was if and only if we know that if $s = 1$ then k must be congruent to 2 or 3 mod 4.

We can now determine when a binary string with k ones satisfies the following conditions for the values of (t, s)

$$\begin{array}{lll} (0,0) & if & k \equiv 0 \bmod 4 \\ (1,0) & if & k \equiv 1 \bmod 4 \\ (0,1) & if & k \equiv 2 \bmod 4 \\ (1,1) & if & k \equiv 3 \bmod 4. \end{array}$$

We can simplify this into one expression

$$(t,s) \quad if \quad k \equiv t + 2s \bmod 4.$$

To count the total number of binary strings that satisfy (t, s) we count all possible ways to have k ones in a binary string of length n and then sum over all possible values for k.

$$\begin{aligned} |\{a_0 a_1 \cdots a_{n-1} \in \{0,1\}^n : \sum_{0\le i<n} a_i = t, \sum_{0\le i<j<n} a_i a_j = s\}| &= \sum_{k\equiv t+2s} \binom{n}{k} \\ &= S_{t+2s}(n). \end{aligned}$$

□

The following lemma expresses the subtrace of a field element as the sum of traces of certain of its powers.

LEMMA 8 *Let $\beta \in \mathrm{GF}(2^n)$. If $n = 2m$ is even, then*

$$St(\beta) = Tr(\beta^3) + Tr(\beta^5) + Tr(\beta^9) + \cdots + Tr(\beta^{2^{m-1}+1}) + Tr_{2^m}(\beta^{2^m+1}).$$

If $n = 2m + 1$ is odd, then

$$St(\beta) = Tr(\beta^3) + Tr(\beta^5) + Tr(\beta^9) + \cdots + Tr(\beta^{2^m+1}).$$

Proof We prove only the case where n is even; the other case is simpler and similar. First note that

$$St(\beta) = \sum_{0\leq i<j<n} \beta^{2^i}\beta^{2^j} = \sum_{s=1}^{n-1}\sum_{t=0}^{n-s-1} \beta^{2^t}\beta^{2^{s+t}}.$$

Break up the latter sum into three parts, depending on whether $s < m$, $s = m$, or $s > m$, and call the respective sums A, B, and C. We deal with B first.

$$B = \sum_{t=0}^{n-m-1} \beta^{2^t}\beta^{2^{m+t}} = \sum_{t=0}^{m-1}(\beta^{2^m+1})^{2^t} = \mathrm{Tr}_{2^m}(\beta^{2^m+1}).$$

Now note that we can write C as

$$\begin{aligned} C &= \sum_{s=m+1}^{n-1}\sum_{t=0}^{n-s-1} \beta^{2^t}\beta^{2^{s+t}} \\ &= \sum_{k=1}^{n-m-1}\sum_{t=0}^{k-1}\beta^{2^t}\beta^{2^{n-k+t}} \\ &= \sum_{s=1}^{m-1}\sum_{t=0}^{s-1}\beta^{2^t}\beta^{2^{n-s+t}} \\ &= \sum_{s=1}^{m-1}\sum_{t=n-s}^{n-1} \beta^{2^{s+t-n}}\beta^{2^t}. \end{aligned}$$

Observe that $\beta^{2^{s+t-n}} = \beta^{2^{s+t}}$. Combining this observation and the last expression for C, we now compute $A + C$.

$$\begin{aligned} A + C &= \sum_{s=1}^{m-1}\sum_{t=0}^{n-s-1} \beta^{2^{s+t}}\beta^{2^t} + \sum_{s=1}^{m-1}\sum_{t=n-s}^{n-1} \beta^{2^{s+t}}\beta^{2^t} \\ &= \sum_{s=1}^{m-1}\sum_{t=0}^{n-1}(\beta^{2^s+1})^{2^t} \\ &= \sum_{s=1}^{m-1}\mathrm{Tr}(\beta^{2^s+1}) \end{aligned}$$

Thus $A + B + C$ is equal to the expression in the statement of the lemma. □

As mentioned, the first two cases in the proof of Theorem 4 utilize a self-dual normal basis for GF(2^n) over GF(2). In each case, the trace and subtrace of an element $\beta \in \mathrm{GF}(2^n)$ are expressed as simple functions of the basis multipliers. The following lemma gives the expression for trace.

LEMMA 9 *Let $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ be a self-dual normal basis, and suppose $\beta = a_0\alpha + \alpha_1\alpha^2 + \cdots + a_{n-1}\alpha^{2^{n-1}}$. Then*

$$Tr(\beta) = \sum_{0 \leq i < n} a_i.$$

Proof Note that $Tr(\alpha) = 1$, since otherwise the basis vectors are linearly dependent. Using basic properties of trace,

$$\begin{aligned} Tr(\beta) &= Tr(\sum_{0 \leq i < n} a_i\alpha^{2^i}) \\ &= \sum_{0 \leq i < n} a_i Tr(\alpha^{2^i}) \\ &= \sum_{0 \leq i < n} a_i. \end{aligned}$$

□

In the following three subsections we prove Theorem 4.

Case 1: n odd

THEOREM 5 *Let n be odd. Let $B = \{\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{n-1}}\}$ be a self-dual normal basis of* GF(2^n) *over* GF(2). *Let $\beta = a_0\alpha + a_1\alpha^2 + a_2\alpha^4 + \ldots + a_{n-1}\alpha^{2^{n-1}}$ be an element of* GF(2^n). *Then*

$$St(\beta) = \sum_{0 \leq i < j < n} a_i a_j.$$

Proof Let $n = 2m + 1$. To apply Lemma 8, we require the trace of β^{2^k+1} for $k = 1, \ldots, m$. Define $a_{-r} = a_{(-r \bmod n)}$ and consider β^{2^k+1}:

$$\begin{aligned} \beta\beta^{2^k} &= (a_0\alpha + a_1\alpha^2 + a_2\alpha^4 + \cdots + a_{n-2}\alpha^{2^{n-2}} + a_{n-1}\alpha^{2^{n-1}}) \\ &\quad (a_{n-k}\alpha + a_{n-k+1}\alpha^2 + a_{n-k+2}\alpha^4 + \cdots + a_{n-k-2}\alpha^{2^{n-2}} + a_{n-k-1}\alpha^{2^{n-1}}) \\ &= \sum_{0 \leq i,j < n} a_i a_{j-k}\alpha^{2^i}\alpha^{2^j}. \end{aligned}$$

When we calculate the trace of β^{2^k+1}, all terms of the form $\alpha^{2^i}\alpha^{2^j}$ with $i \neq j$ are zero, as B is self-dual. Thus the trace of β^{2^k+1} is given by

$$\begin{aligned} Tr(\beta^{2^k+1}) &= Tr(\sum_{0\leq i<n} a_i a_{i-k}\alpha^{2^i}\alpha^{2^i}) \\ &= \sum_{0\leq i<n} a_i a_{i-k} Tr(\alpha^{2^{i+1}}) \\ &= \sum_{0\leq i<n} a_i a_{i-k} \\ &= \sum_{\substack{i<j \\ j-i=k}} a_i a_j + \sum_{\substack{i<j \\ j-i=n-k}} a_i a_j. \end{aligned}$$

Applying Lemma 8, we sum the last expression for $k = 1, 2, \ldots, m$.

$$\begin{aligned} St(\beta) &= \sum_{k=1}^{m} \left[\sum_{\substack{i<j \\ j-i=k}} a_i a_j + \sum_{\substack{i<j \\ j-i=n-k}} a_i a_j \right] \\ &= \sum_{\substack{i<j \\ 1\leq j-i\leq m}} a_i a_j + \sum_{\substack{i<j \\ n-m\leq j-i<n}} a_i a_j \\ &= \sum_{0\leq i<j<n} a_i a_j. \end{aligned}$$

□

The following corollary follows from the preceding theorem and Lemma 9.

COROLLARY 2 *Let n be odd. The number of elements $\beta \in$ GF(2^n) with $Tr(\beta) = t$ and $St(\beta) = s$ equals the number of n-tuples $[a_0, a_1, \ldots, a_{n-1}] \in$ GF$(2)^n$ with*

$$\sum_{0\leq i<j<n} a_i = t \quad \textit{and} \quad \sum_{0\leq i<j<n} a_i a_j = s.$$

Thus, by Lemma 7 we have now proved Theorem 4 for the case when n is odd.

Case 2: $n \equiv 2 \bmod 4$

This section deals with the case of n even, but not a multiple of 4. As with the n odd case, it relies on the existence of a self-dual normal basis.

Some preliminary material, culminating in Corollary 3, is needed to show a property of the basis generator α. Throughout this section, $n = 2m$, where m is odd.

LEMMA 10 *If n is even, and $\alpha \in \mathrm{GF}(2^n)$ with $Tr(\alpha) = 1$ then $Tr_{2^n:4}(\alpha)Tr_{2^n:4}(\alpha^2) = 1$.*

Proof Let $\theta = Tr_{2^n:4}(\alpha)$, $\theta \in \mathrm{GF}(4)$, so that

$$\begin{aligned} \theta &= \alpha + \alpha^4 + \alpha^{16} + \cdots + \alpha^{2^{n-2}} \quad \text{and} \\ \theta^2 &= \alpha^2 + \alpha^8 + \alpha^{32} + \cdots + \alpha^{2^{n-1}}. \end{aligned}$$

Then $Tr_{2^n:4}(\alpha)Tr_{2^n:4}(\alpha^2) = \theta^3$, and thus is either 0 or 1. If $\theta^3 = 0$, then $\theta = \theta^2 = 0$, but $\theta + \theta^2 = Tr(\alpha) = 1$, a contradiction. □

LEMMA 11 *If $n \equiv 2 \bmod 4$, $m = n/2$, and $\alpha \in \mathrm{GF}(2^n)$ then*

$$Tr_{2^n:4}(\alpha)Tr_{2^n:4}(\alpha^2) = \sum_{k=1}^{(m-1)/2} Tr(\alpha^{2^{2k-1}+1}) + Tr_{2^m}(\alpha^{2^m+1}).$$

Proof Note that $\alpha^{2^m+1} \in \mathrm{GF}(2^m)$ since $(\alpha^{2^m+1})^{2^m} = \alpha^{2^m+1}$, so that the trace expression $Tr_{2^m}(\alpha^{2^m+1})$ is well-defined.

$$\begin{aligned} Tr_{2^n:4}(\alpha)Tr_{2^n:4}(\alpha^2) &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \alpha^{2^{2i}}\alpha^{2^{2j+1}} \\ &= \sum_{i=0}^{m-1}\sum_{j=i}^{m-1} \alpha^{2^{2i}}\alpha^{2^{2j+1}} + \sum_{i=0}^{m-1}\sum_{j=0}^{i-1} \alpha^{2^{2i+1}}\alpha^{2^{2j+2m+1}} \\ &= \sum_{i=0}^{m-1}\sum_{j=i}^{m-1} \alpha^{2^{2i}}\alpha^{2^{2j+1}} + \sum_{i=0}^{m-1}\sum_{j=m}^{m+i-1} \alpha^{2^{2i}}\alpha^{2^{2j+1}} \\ &= \sum_{i=0}^{m-1}\sum_{j=i}^{m+i-1} \alpha^{2^{2i}}\alpha^{2^{2j+1}} \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \alpha^{2^{2i}}\alpha^{2^{2(i+j)+1}} \\ &= \sum_{j=0}^{m-1} D_j, \end{aligned}$$

where

$$D_j = \sum_{i=0}^{m-1} \alpha^{2^{2i}} \alpha^{2^{2(i+j)+1}} = \sum_{i=0}^{m-1} (\alpha^{2^{2j+1}+1})^{2^{2i}}. \tag{19}$$

Note that

$$Tr_{2^n:4}(\alpha) Tr_{2^n:4}(\alpha^2) = D_{(m-1)/2} + \sum_{j=0}^{(m-3)/2} (D_j + D_{m-j-1}). \tag{20}$$

To simplify this expression we re-arrange the sum for D_{m-j-1} as follows:

$$\begin{aligned} D_{m-j-1} &= \sum_{i=0}^{j} \alpha^{2^{2(i+m-j-1)+1}} \alpha^{2^{2i}} + \sum_{i=j+1}^{m-1} \alpha^{2^{2(i+m-j-1)+1}} \alpha^{2^{2i}} \\ &= \sum_{k=m-j-1}^{m-1} \alpha^{2^{2k+1}} \alpha^{2^{2(k+j+1)}} + \sum_{k=0}^{m-j-2} \alpha^{2^{2k+1}} \alpha^{2^{2(k+j+1)}} \\ &= \sum_{k=0}^{m-1} \alpha^{2^{2k+1}} \alpha^{2^{2(k+j+1)}} \\ &= \sum_{k=0}^{m-1} (\alpha^{2^{2j+1}+1})^{2^{2k+1}}. \end{aligned}$$

Thus,

$$\begin{aligned} D_j + D_{m-j-1} &= \sum_{i=0}^{m-1} \alpha^{2^{2i}} \alpha^{2^{2(i+j+1)}} + \sum_{i=0}^{m-1} \alpha^{2^{2i+1}} \alpha^{2^{2(i+j+1)}} \\ &= \sum_{i=0}^{n-1} \alpha^{2^i} \alpha^{2^{2(i+j+1)}} \\ &= Tr(\alpha^{2^{2j+1}+1}). \end{aligned} \tag{21}$$

It only remains to calculate $D_{(m-1)/2}$.

$$\begin{aligned}
D_{(m-1)/2} &= \sum_{i=0}^{m-1} \alpha^{2^{2i}} \alpha^{2^{2i+m}} \\
&= \sum_{i=0}^{(m-1)/2} \alpha^{2^{2i}} \alpha^{2^{2i+m}} + \sum_{i=(m+1)/2}^{m-1} \alpha^{2^{2i}} \alpha^{2^{2i+m}} \\
&= \sum_{i=0}^{(m-1)/2} \alpha^{2^{2i}} \alpha^{2^{2i+m}} + \sum_{i=0}^{(m-3)/2} \alpha^{2^{2i+m+1}} \alpha^{2^{2i+1}} \\
&= \sum_{i=0}^{(m-1)/2} (\alpha^{2^m+1})^{2^{2i}} + \sum_{i=0}^{(m-3)/2} (\alpha^{2^m+1})^{2^{2i+1}} \\
&= \sum_{i=0}^{m-1} (\alpha^{2^m+1})^{2^i} \\
&= Tr_{2^m}(\alpha^{2^m+1}). \qquad (22)
\end{aligned}$$

Substituting (21) and (22) into expression (20) finishes the proof. □

COROLLARY 3 *If* $n \equiv 2 \bmod 4$, $m = n/2$, *and* $\alpha \in \mathrm{GF}(2^n)$ *generates a self-dual normal basis then*

$$Tr_{2^m}(\alpha^{2^m+1}) = 1.$$

Proof Since α generates a self-dual normal basis, $Tr(\alpha) = 1$ and $Tr(\alpha^{2^{2k-1}+1}) = 0$ for all k, and so

$$1 = Tr_{2^n:4}(\alpha) Tr_{2^n:4}(\alpha^2) = Tr_{2^m}(\alpha^{2^m+1}).$$

□

THEOREM 6 *Let* n *be even. Let* $B = \{\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{n-1}}\}$ *be a self-dual normal basis of* $\mathrm{GF}(2^n)$ *over* $\mathrm{GF}(2)$*. Let* $\beta = a_0\alpha + a_1\alpha^2 + a_2\alpha^4 + \ldots + a_{n-1}\alpha^{2^{n-1}}$ *be an element of* $\mathrm{GF}(2^n)$*. Then*

$$St(\beta) = \sum_{0 \le i < j < n} a_i a_j + \sum_{0 \le i < n} a_i.$$

Proof The subtrace relates to the trace as follows:

$$St(\beta) = Tr(\beta^3) + Tr(\beta^5) + \cdots + Tr(\beta^{2^{m-1}+1}) + Tr_{2^m}(\beta^{2^m+1}) \qquad (23)$$

where $m = n/2$. Note that as $2^m(2^m+1) = 2^m + 1(\mathrm{mod} 2^n - 1)$ the mth conjugate of β^{2^m+1} is itself, and so β^{2^m+1} is an element of GF(2^m). Now consider β^{2^k+1}:

$$\beta^{2^k+1} = \sum_{0 \le i,j < n} a_i a_{j-k} \alpha^{2^i} \alpha^{2^j}.$$

When we calculate the trace of β^{2^k+1}, $k < m$, all terms of the form $\alpha^{2^i}\alpha^{2^j}$ with $i \neq j$ are zero, as B is self-dual. Thus the trace of β^{2^k+1} is given by

$$\begin{aligned} Tr(\beta^{2^k+1}) &= Tr(\sum_{0 \le i < n} a_i a_{i-k} \alpha^{2^i} \alpha^{2^i}) \\ &= \sum_{0 \le i < n} a_i a_{i-k} Tr(\alpha^{2^{i+1}}) \\ &= \sum_{0 \le i < n} a_i a_{i-k} \\ &= \sum_{\substack{i<j \\ j-i=k}} a_i a_j + \sum_{\substack{i<j \\ j-i=n-k}} a_i a_j. \end{aligned}$$

Now, consider β^{2^m+1}:

$$\beta^{2^m+1} = \sum_{0 \le i,j < n} a_i a_{j-m} \alpha^{2^i} \alpha^{2^j}.$$

Separating the terms for which $j = i$ and those for which $j = i + m$,

$$\beta^{2^m+1} = C + D + E$$

where

$$\begin{aligned} C &= \sum_{0 \le i < n} a_i a_{i-m} \alpha^{2^{i+1}} \text{ and} \\ D &= \sum_{0 \le i < n} a_i a_i \alpha^{2^i} \alpha^{2^{i+m}}. \end{aligned}$$

The terms in E are paired by the bijection on the indices $(i,j) \leftrightarrow (j+m, i+m)$. A pair of such terms has the form

$$a_i a_{j+m} \alpha^{2^i} \alpha^{2^j} + a_{j+m} a_i \alpha^{2^{j+m}} \alpha^{2^{i+m}} = a_i a_{j+m} (\alpha^{2^i} \alpha^{2^j} + \alpha^{2^{i+m}} \alpha^{2^{j+m}}).$$

The trace in GF(2^m) of this pair is

$$a_i a_{j+m} Tr_{2^m}(\alpha^{2^i} \alpha^{2^j} + \alpha^{2^{i+m}} \alpha^{2^{j+m}}) = a_i a_{j+m} Tr(\alpha^{2^i} \alpha^{2^j}) = 0.$$

as B is self-dual.

Now consider the trace in GF(2^m) of D:

$$\begin{aligned}
Tr_{2^m}(D) &= Tr_{2^m}(\sum_{0\leq i<n} a_i a_i \alpha^{2^i}\alpha^{2^{i+m}}) \\
&= Tr_{2^m}(\sum_{0\leq i<n} a_i(\alpha\alpha^{2^m})^{2^i}) \\
&= \sum_{0\leq i<n} a_i Tr_{2^m}(\alpha^{2^m+1})^{2^i} \\
&= \sum_{0\leq i<n} a_i Tr_{2^m}(\alpha^{2^m+1}).
\end{aligned}$$

By Corollary 3, $Tr_{2^m}(\alpha^{2^m+1}) = 1$, and so

$$Tr_{2^m}(D) = \sum_{0\leq i\leq n-1} a_i.$$

This leaves us with $Tr_{2^m}(C)$:

$$Tr_{2^m}(C) = \sum_{0\leq i\leq n-1} Tr_{2^m}(a_i a_{i-m}\alpha^{2^{i+1}}).$$

Pairing the terms by the bijection on indices $i \leftrightarrow i+m$ gives

$$\begin{aligned}
Tr_{2^m}(C) &= \sum_{0\leq i<m} Tr_{2^m}(a_i a_{i+m}\alpha^{2^{i+1}}) + Tr_{2^m}(a_{i+m} a_i \alpha^{2^{i+m+1}}) \\
&= \sum_{0\leq i<m} a_i a_{i+m} Tr_{2^m}(\alpha^{2^{i+1}} + \alpha^{2^{i+m+1}}) \\
&= \sum_{0\leq i<m} a_i a_{i+m} Tr(\alpha^{2^{i+1}}) \\
&= \sum_{0\leq i<m} a_i a_{i+m}
\end{aligned}$$

again, as B is self-dual. Thus,

$$Tr_{2^m}(\beta^{2^m+1}) = \sum_{0\leq i<m} a_i a_{i+m} + \sum_{0\leq i<n} a_i.$$

Applying Lemma 8,

$$\begin{aligned} St(\beta) &= \sum_{k=1}^{m-1} Tr(\beta^k) + Tr_{2^m}(\beta^{2^m+1}) \\ &= \sum_{k=1}^{m-1} \left(\sum_{\substack{i<j \\ j-i=k}} a_i a_j + \sum_{\substack{i<j \\ j-i=n-k}} a_i a_j \right) + \sum_{0 \leq i<m} a_i a_{i+m} + \sum_{0 \leq i<n} a_i \\ &= \sum_{\substack{i<j \\ 1 \leq j-i \leq m}} a_i a_j + \sum_{\substack{i<j \\ n-m \leq j-i<n}} a_i a_j + \sum_{0 \leq i<m} a_i a_{i+m} + \sum_{0 \leq i<n} a_i \\ &= \sum_{0 \leq i<j<n} a_i a_j + \sum_{0 \leq i<n} a_i. \end{aligned}$$

□

The following corollary follows from the preceding theorem and Lemma 9.

COROLLARY 4 *Let* $n \equiv 2 \bmod 4$. *The number of elements* $\beta \in \mathrm{GF}(2^n)$ *with* $Tr(\beta) = t$ *and* $St(\beta) = s$ *equals the number of* n*-tuples* $[a_0, a_1, \ldots, a_{n-1}] \in \mathrm{GF}(2^n)$ *with*

$$\sum_{0 \leq i<j<n} a_i = t \quad \textit{and} \quad \sum_{0 \leq i<j<n} a_i a_j = s + t.$$

By Lemma 7, we have now shown that $F(n, s, t) = S_{t+2(s+t \bmod 2)}(n)$. This agrees with the expression of Theorem 7 if $t = 1$, but not if $t = 0$. However, note that if $n \equiv 2$, then $S_0(n) = S_2(n)$. This follows from the symmetry $\binom{n}{k} = \binom{n}{n-k}$ of the binomial coefficients. Thus $F(n, s, t) = S_{t+2s}(n)$ for either value of t and we have proved Theorem 4 for the case when $n \equiv 2$.

Case 3: $n \equiv 0 \bmod 4$

For all of the below material, n is a multiple of 4, and $m = n/2$. Also, if unspecified, trace and subtrace are of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$.

An overview of this case is as follows. We partition $\mathrm{GF}(2^n)$ into 2^m equivalence classes, each of size 2^m. We then combine two results: (a) half of the classes have all elements trace 0, and half have all elements trace 1; and (b) each of the classes, except for one, consists half of subtrace 0 elements and half of subtrace 1 elements. The exceptional class, which turns out to be the self-complementary elements, is all trace 0, and either all subtrace

0 or all subtrace 1 (depending on n). Thus we can determine the number of trace s subtrace t elements (one half of the elements of one half of the classes, accounting for the exception).

DEFINITION 1 *Let $\alpha \in \mathrm{GF}(2^m)$. Define R_α as $\{\beta \in \mathrm{GF}(2^n) : \beta^{2^m} + \beta = \alpha\}$. Note that R_α is the set of all elements β in* GF(2^n) *with $Tr_{2^n:2^m}(\beta) = \alpha$.*

The following lemma shows that GF(2^n) is partitioned into 2^m classes of size 2^m.

LEMMA 12 *Let $\alpha \in \mathrm{GF}(2^m)$. Then R_α is a coset of* GF(2^m) $\subseteq$ GF(2^n).

Proof If $\beta_1, \beta_2 \in R_\alpha$, then

$$\begin{aligned}(\beta_1 + \beta_2)^{2^m} &= \beta_1^{2^m} + \beta_2^{2^m} \\ &= (\beta_1 + \alpha) + (\beta_2 + \alpha) \\ &= \beta_1 + \beta_2.\end{aligned}$$

Thus $\beta_1 + \beta_2 \in \mathrm{GF}(2^m)$. So each R_α has $|R_\alpha| \geq 2^m$. These sets are disjoint and there are 2^m of them. Thus $|R_\alpha| = 2^m$. □

This lemma shows a useful property of the trace of a product when one of the elements is in GF(2^m).

LEMMA 13 *Let $\beta \in \mathrm{GF}(2^n)$, $\gamma \in \mathrm{GF}(2^m)$. Then $Tr(\beta\gamma^{2^k}) = Tr(\beta^{2^{m-k}}\gamma)$.*

Proof $Tr(\beta\gamma^{2^k}) = Tr((\beta\gamma^{2^k})^{2^{m-k}}) = Tr((\beta^{2^{m-k}}\gamma^{2^m})) = Tr((\beta^{2^{m-k}}\gamma))$ since $\gamma \in \mathrm{GF}(2^m)$. □

The following is the central result. It shows that there is usually an additive "subtrace-changing" element in GF(2^m).

LEMMA 14 *Let $\alpha \in \mathrm{GF}(2^m)$. Let $\gamma \in \mathrm{GF}(2^m)$ with $Tr_{2^m}((\alpha + 1)\gamma) = 1$. Let $\beta \in R_\alpha$. Then $St(\beta + \gamma) = St(\beta) + 1$.*

Proof By Lemma 8,

$$\begin{aligned}
St(\beta+\gamma) &= \sum_{k=1}^{m-1} Tr((\beta+\gamma)^{2^k+1}) + Tr_{2^m}((\beta+\gamma)^{2^m+1}) \\
&= \sum_{k=1}^{m-1} Tr((\beta+\gamma)^{2^k}(\beta+\gamma)) + Tr_{2^m}((\beta+\gamma)^{2^m}(\beta+\gamma)) \\
&= \sum_{k=1}^{m-1} Tr(\beta^{2^k+1} + \beta^{2^k}\gamma + \beta\gamma^{2^k} + \gamma^{2^k+1}) \\
&\quad + Tr_{2^m}(\beta^{2^m+1} + \beta^{2^m}\gamma + \beta\gamma^{2^m} + \gamma^{2^m+1}).
\end{aligned}$$

If we calculate $St(\beta+\gamma)+St(\beta)$, the terms involving just β cancel, and so

$$\begin{aligned}
St(\beta+\gamma)+St(\beta) &= \sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma + \beta\gamma^{2^k} + \gamma^{2^k+1}) + \\
&\quad Tr_{2^m}(\beta^{2^m}\gamma + \beta\gamma^{2^m} + \gamma^{2^m+1}).
\end{aligned}$$

Since $\gamma \in \mathrm{GF}(2^m)$, the terms involving the trace of powers of γ are 0, and so

$$\begin{aligned}
St(\beta+\gamma)+St(\beta) &= \sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma + \beta\gamma^{2^k}) + \\
&\quad Tr_{2^m}(\beta^{2^m}\gamma + \beta\gamma^{2^m} + \gamma^{2^m+1}).
\end{aligned}$$

Now consider the summation. By Lemma 13,

$$\begin{aligned}
\sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma + \beta\gamma^{2^k}) &= \sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma + \beta^{2^{m-k}}\gamma) \\
&= \sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma) + \sum_{k=1}^{m-1} Tr(\beta^{2^{m-k}}\gamma) \\
&= \sum_{k=1}^{m-1} Tr(\beta^{2^k}\gamma) + \sum_{l=1}^{m-1} Tr(\beta^{2^l}\gamma) \\
&= 0,
\end{aligned}$$

and so

$$\begin{aligned}
St(\beta+\gamma)+St(\beta) &= Tr_{2^m}(\beta^{2^m}\gamma+\beta\gamma^{2^m}+\gamma^{2^m+1})\\
&= Tr_{2^m}(\alpha\gamma)+Tr_{2^m}(\gamma^{2^m+1})\\
&= Tr_{2^m}(\alpha\gamma)+Tr_{2^m}(\gamma^{2})\\
&= Tr_{2^m}(\alpha\gamma)+Tr_{2^m}(\gamma)\\
&= Tr_{2^m}(\alpha\gamma+\gamma)\\
&= Tr_{2^m}((\alpha+1)\gamma)\\
&= 1.
\end{aligned}$$

Thus, $St(\beta+\gamma)+St(\beta)=1$, or $St(\beta+\gamma)=St(\beta)+1$. □

Note that if $\alpha = 1$, then no such γ exists.

The next lemma points out that the additive subtrace-changing element splits each class (except one) into two halves.

LEMMA 15 *The coset R_α, $\alpha \neq 1$, contains 2^{m-1} elements with subtrace 0, and 2^{m-1} elements with subtrace 1.*

Proof Let $\alpha \in \mathrm{GF}(2^m)$, and suppose $\alpha \neq 1$. Since $(\alpha+1)\cdot\mathrm{GF}(2^m) = \mathrm{GF}(2^m)$ and $\mathrm{GF}(2^m)$ contains 2^{m-1} elements with trace 1, there exists an element $\gamma \in \mathrm{GF}(2^m)$ with $Tr((\alpha+1)\gamma) = 1$.

Since R_α is a coset, it is closed under addition by γ. By this and Lemma 14, addition by γ is a bijection between the subtrace 0 and the subtrace 1 elements of R_α. Thus these two sets are equal-sized, with size 2^{m-1}. □

We now focus on the exceptional class: the self-complementary elements.

LEMMA 16 *Let $\beta \in R_1$. Then $St(\beta) = \llbracket n \equiv 0 \bmod 8 \rrbracket$.*

Proof The set R_1 consists of all roots of all self-complementary irreducible polynomials of degree n/d, where d is odd. Let $\beta \in R_1$, and let p be the minimal polynomial of β, with degree of $p = k = n/d$. From [3], k is even. From Lemma 4 and equation (14), $St(\beta) = St(p^d) = d{\cdot}St_{2^k}(p) + \binom{d}{2}Tr_{2^k}(p)$.

If $n \equiv 4 \bmod 8$, then d odd implies $k \equiv 4 \bmod 8$. From Theorem 4 of [3], $Tr_{2^k}(p) = St_{2^k}(p) = 0$, and so $St(\beta) = 0$.

If $n \equiv 0 \bmod 8$, then d odd implies $k \equiv 0 \bmod 8$. From Theorem 4 of [3], $Tr_{2^k}(p) = 0$ and $St_{2^k}(p) = 1$, and so $St(\beta) = d$. Since d is odd, $St(\beta) = 1$. □

The following three lemmata account for the distribution of GF(2^n) in terms of trace.

LEMMA 17 *Let $\beta \in R_\alpha$. Then $Tr(\beta) = Tr_{2^m}(\alpha)$. That is, all elements in the coset of α have trace $Tr_{2^m}(\alpha)$.*

Proof

$$\begin{aligned} Tr(\beta) &= \beta + \beta^2 + \beta^4 + \cdots + \beta^{2^{n-1}} \\ &= (\beta + \beta^{2^m}) + (\beta^2 + \beta^{2^{m+1}}) + \cdots + (\beta^{2^{m-1}} + \beta^{2^{2m-1}}) \\ &= (\beta + \beta^{2^m}) + (\beta + \beta^{2^m})^2 + \cdots + (\beta + \beta^{2^m})^{2^{m-1}} \\ &= \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}} \\ &= Tr_{2^m}(\alpha). \end{aligned}$$

□

Thus we can unambiguously define of the *trace of the coset R_α*, $Tr(R_\alpha) = Tr_{2^m}(\alpha)$.

LEMMA 18 *Of the 2^m cosets, 2^{m-1} have all elements having trace 0, and 2^{m-1} have all elements having trace 1.*

Proof In GF(2^m), $|\{\alpha : Tr_{2^m}(\alpha) = 0\}| = 2^{m-1}$. □

LEMMA 19 $Tr(R_1) = 0$.

Proof The trace of 1 in an extension of even-degree is 0. □

THEOREM 7 *The number of elements in* GF(2^n) *with given trace and subtrace are as follows.*

	t	s	$F(n,t,s)$
	0	*0*	$2^{n-2} - 2^{m-1}$
If $8\|n$:	*0*	*1*	$2^{n-2} + 2^{m-1}$
	1	*0*	2^{n-2}
	1	*1*	2^{n-2}

	t	s	$F(n,t,s)$
	0	*0*	$2^{n-2} + 2^{m-1}$
If $8 \not\| n$:	*0*	*1*	$2^{n-2} - 2^{m-1}$
	1	*0*	2^{n-2}
	1	*1*	2^{n-2}

Proof First consider the 2^{m-1} cosets with trace 1 (Lemma 18). As R_1 is not among these (Lemma 19), each has 2^{m-1} subtrace 0 elements and

2^{m-1} subtrace 1 elements. (Lemma 15). Thus $F(n,1,0)$ and $F(n,1,1)$ are both $2^{2m-2} = 2^{n-2}$.

Similarly, consider the $2^{m-1} - 1$ cosets with trace 0, excluding R_1. In the union of these cosets, the number of trace 1 subtrace 0 elements and the number of trace 1 subtrace 1 elements is $(2^{m-1} - 1)2^{m-1} = 2^{n-2} - 2^{m-1}$.

If $8|n$, then by Lemma 16, all the elements of R_1 have subtrace 1, and so $F(n,0,1) = 2^{n-2} - 2^{m-1} + 2^m = 2^{n-2} + 2^{m-1}$, and $F(n,0,0)$, unaffected by R_1, is $2^{n-2} - 2^{m-1}$.

If $8 \not| n$, then the elements in R_1 have subtrace 0, again giving the desired numbers. □

Comparing Theorem 7 with Lemma 7 we see that $F(n,t,s) = S_{t+2\bar{s}}(n)$, thereby proving Theorem 4 when $n \equiv 2$. The proof of Theorem 4 is now complete.

5 Proof of Main Theorem

Applying the Möbius inversion of Theorem 1 to equations (15) and (16) we obtain

$$\begin{aligned} n \cdot P(n,1,0) \quad = \quad & \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) \left[\sum_{\substack{i\equiv 1 \\ n/d \text{ odd}}} \binom{n/d}{i} + \sum_{\substack{i\equiv 3 \\ n/d \text{ even}}} \binom{n/d}{i} \right] + \\ & \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) \left[\sum_{\substack{i\equiv 3 \\ n/d \text{ odd}}} \binom{n/d}{i} + \sum_{\substack{i\equiv 1 \\ n/d \text{ even}}} \binom{n/d}{i} \right] \end{aligned}$$

$$
\begin{aligned}
= \; & \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) \sum_{\substack{i,k \\ n/d \text{ odd}}} \binom{n/d}{k/d} \llbracket id = k \rrbracket \llbracket i \equiv 1 \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) \sum_{\substack{i,k \\ n/d \text{ odd}}} \binom{n/d}{k/d} \llbracket id = k \rrbracket \llbracket i \equiv 3 \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) \sum_{\substack{i,k \\ n/d \text{ even}}} \binom{n/d}{k/d} \llbracket id = k \rrbracket \llbracket i \equiv 3 \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) \sum_{\substack{i,k \\ n/d \text{ even}}} \binom{n/d}{k/d} \llbracket id = k \rrbracket \llbracket i \equiv 1 \rrbracket \\
= \; & \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) \sum_{\substack{d|k \\ k\equiv 1}} \binom{n/d}{k/d} \llbracket n/d \text{ odd} \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) \sum_{\substack{d|k \\ k\equiv 1}} \binom{n/d}{k/d} \llbracket n/d \text{ odd} \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) \sum_{\substack{d|k \\ k\equiv 3}} \binom{n/d}{k/d} \llbracket n/d \text{ even} \rrbracket + \\
& \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) \sum_{\substack{d|k \\ k\equiv 3}} \binom{n/d}{k/d} \llbracket n/d \text{ even} \rrbracket \\
= \; & \llbracket n \text{ odd} \rrbracket \sum_{k\equiv 1} \sum_{d|\gcd(n,k)} \mu(d) \binom{n/d}{k/d} \; + \\
& \llbracket n \text{ even} \rrbracket \sum_{k\equiv 3} \sum_{d|\gcd(n,k)} \mu(d) \binom{n/d}{k/d} \\
= \; & \llbracket n \text{ odd} \rrbracket \sum_{k\equiv 1} n \cdot L(n,k) \; + \; \llbracket n \text{ even} \rrbracket \sum_{k\equiv 3} n \cdot L(n,k).
\end{aligned}
$$

This establishes the result for $P(n,1,0)$. The derivation of the result for $P(n,1,1)$ is almost identical and is omitted.

The result for $P(n,0,0)$ is obtained by applying the Möbius inversion of Corollary 1 to equation (17).

$$n \cdot P(n,0,0) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) \left[\sum_{\substack{i \equiv 0 \\ n/d \text{ odd}}} \binom{n/d}{i} + \sum_{\substack{i \equiv 2 \\ n/d \text{ even}}} \binom{n/d}{i} - [\![n/d \text{ even}]\!] 2^{n/2d-1} \right]$$

Since d is odd, n/d is odd when n is odd and n/d is even when n is even. In the case where n is odd we obtain

$$\begin{aligned} n \cdot P(n,0,0) &= \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) \sum_{\substack{d|k \\ k \equiv 0}} \binom{n/d}{k/d} \\ &= \sum_{k \equiv 0} \sum_{d|\gcd(n,k)} \mu(d) \binom{n/d}{k/d} \\ &= \sum_{k \equiv 0} n \cdot L(n,k). \end{aligned}$$

In the case were n is even we obtain

$$\begin{aligned} n \cdot P(n,0,0) &= \sum_{\substack{d|n \\ d \text{ odd}}} \left[\mu(d) \sum_{\substack{d|k \\ k \equiv 2}} \binom{n/d}{k/d} - \mu(d) 2^{n/2d-1} \right] \\ &= \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) \sum_{\substack{d|k \\ k \equiv 2}} \binom{n/d}{k/d} + \sum_{\substack{d|n \\ d \text{ odd}}} \mu(2d) 2^{n/2d-1} \\ &= \sum_{k \equiv 2} \sum_{\substack{d|\gcd(n,k) \\ d \text{ odd}}} \mu(d) \binom{n/d}{k/d} + \sum_{\substack{d|n \\ d \equiv 2}} \mu(d) 2^{n/d-1} \\ &= \sum_{k \equiv 2} \sum_{\substack{d|\gcd(n,k) \\ d \text{ odd}}} \mu(d) \binom{n/d}{k/d} + \sum_{\substack{d|n \\ d \equiv 2}} \mu(d) \sum_{m \text{ odd}} \binom{n/d}{m} \\ &= \sum_{k \equiv 2} \sum_{\substack{d|\gcd(n,k) \\ d \text{ odd}}} \mu(d) \binom{n/d}{k/d} + \\ & \quad \sum_{d|n} \sum_{m,k} \mu(d) \binom{n/d}{m} [\![dm = k]\!] [\![d \equiv 2]\!] [\![m \text{ odd}]\!] \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k\equiv 2} \sum_{\substack{d \mid \gcd(n,k) \\ d \text{ odd}}} \mu(d)\binom{n/d}{k/d} + \\
&\quad \sum_{d\mid n} \sum_{m,k} \mu(d)\binom{n/d}{m} [\![dm = k]\!][\![dm \equiv 2]\!][\![d \text{ even}]\!] \\
&= \sum_{k\equiv 2} \sum_{\substack{d \mid \gcd(n,k) \\ d \text{ odd}}} \mu(d)\binom{n/d}{k/d} + \sum_{\substack{d\mid n \\ d \text{ even}}} \sum_{\substack{d\mid k \\ k\equiv 2}} \mu(d)\binom{n/d}{k/d} \\
&= \sum_{k\equiv 2} \sum_{\substack{d \mid \gcd(n,k) \\ d \text{ odd}}} \mu(d)\binom{n/d}{k/d} + \sum_{k\equiv 2} \sum_{\substack{d \mid \gcd(n,k) \\ d \text{ even}}} \mu(d)\binom{n/d}{k/d} \\
&= \sum_{k\equiv 2} n \cdot L(n,k).
\end{aligned}
$$

This establishes the result for $P(n,0,0)$. The derivation of the result for $P(n,0,1)$ is almost identical and is omitted. □

References

[1] L. Carlitz, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. reine angew. Math., 227 (1967) 212-220.

[2] K. Cattell, C.R. Miers, F. Ruskey, J. Sawada, and M. Serra, *Much Odd Enumeration*, manuscript, 1998.

[3] K. Cattell, C.R. Miers, F. Ruskey, and J. Sawada, *The number of self-complementary irreducible polynomials over GF(2)*, manuscript, 1998.

[4] E.N. Gilbert and J. Riordan, *Symmetry Types of Periodic Sequences*, Illinois J. Mathematics, 657-665.

[5] S.W. Golomb, *Shift Register Sequences*, Holden-Day, 1967.

[6] Dieter Jungnickel, *Finite Fields: structure and arithmetics*, B.I. Wissenschaftsverlag, 1993.

[7] D.E. Knuth, R.L. Graham, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.

[8] E.N. Kuz'min, *On a class of irreducible polynomials over a finite field*, (Russian) Dokl. Akad. Nauk SSSR 313 (1990), No. 3, 552-555; translation in Soviet Math. Dokl. 42 (1991) No. 1, 45-48.

[9] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[10] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[11] R.L. Miller, *Necklaces, symmetries, and self-reciprocal polynomials*, Discrete Math., 22 (1978) 25-33.

[12] J.L. Yucas and G.L. Mullen, *Irreducible Polynomials over GF(2) with Prescribed Coefficients*, manuscript, 2001.