Finite Fields and Their Applications 29 (2014) 118–131

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The number of irreducible polynomials over finite fields of characteristic 2 with given trace and subtrace

Won-Ho Ri [*], Gum-Chol Myong, Ryul Kim, Chang-Il Rim

Faculty of Mathematics, Kim Il Sung University, Pyongyang, Democratic People's Republic of Korea

ARTICLE INFO

Article history:
Received 12 December 2013
Received in revised form 15 March 2014
Accepted 10 April 2014
Available online 7 May 2014
Communicated by D. Panario

MSC:
11T06
11A25
12E20

Keywords:
Finite field
Irreducible polynomial
Trace
Möbius inversion formula

ABSTRACT

In this paper we obtained the formula for the number of irreducible polynomials with degree n over finite fields of characteristic two with given trace and subtrace. This formula is a generalization of the result of Cattell et al. (2003) [2].

1. Introduction

In the theory of polynomials over finite fields the existence and the number of irreducible polynomials with some given coefficients have been investigated extensively.

[*] Corresponding author.
E-mail address: riwonho@yahoo.com (W.-H. Ri).

http://dx.doi.org/10.1016/j.ffa.2014.04.003
1071-5797/© 2014 Elsevier Inc. All rights reserved.

Hansen–Mullen conjecture states that for $n \geqslant 3$, there exist irreducible polynomials of degree n over a finite field $\mathrm{GF}(q)$ with any one coefficient given to any element of $\mathrm{GF}(q)$. This conjecture has already been settled completely and generalized to several classes of polynomials over finite fields. See, for example, [5,11,12].

In addition to the existence problem, calculating or estimating the number of irreducible polynomials over finite fields with some given coefficients has been studied by many researchers. It is well known that a formula

$$P(n) = \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d}$$

gives the number of monic irreducible polynomials of degree n over $\mathrm{GF}(q)$, where $\mu(d)$ is the Möbius function [7]. Less well known is the formula

$$P_1(n) = \frac{1}{qn} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d}$$

which counts the number of monic irreducible polynomials of degree n over $\mathrm{GF}(q)$ that have a given nonzero trace [1,2,13,15].

Cattell et al. [2] refined these formulas by enumerating the irreducible polynomials of degree n over $\mathrm{GF}(2)$ with given trace and subtrace. The *trace* of a monic irreducible polynomial $p(x)$ of degree n over $\mathrm{GF}(q)$ is the coefficient of x^{n-1} and the *subtrace* is the coefficient of x^{n-2}. The result obtained in [2] is that the number of degree n irreducible polynomials over $\mathrm{GF}(2)$ with given trace and subtrace is covered by one of the following cases:

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

Here $L(n,k)$ is the number of binary Lyndon words of length n containing exactly k 1's. A binary Lyndon word of length n is an n-character string over an alphabet of size 2 (e.g., 0 and 1), and which is the minimum element in the lexicographical ordering of all its rotations. It is known that

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

In [2], a generalized Möbius Inversion Formula was proved and used [2, Theorem 1].

Yucas and Mullen [14] enumerated the number of irreducible polynomials of even degree over $\mathrm{GF}(2)$ with the first three coefficients prescribed. Fitzgerald and Yucas [3]