Finite Fields and Their Applications 31 (2015) 8–11

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A new proof of Fitzgerald's characterization of primitive polynomials

Samrith Ram

Institut de Mathématiques de Luminy, Luminy Case 907, 13288 Marseille Cedex 9, France

ARTICLE INFO

Article history:
Received 5 June 2014
Received in revised form 27 September 2014
Accepted 29 September 2014
Available online 4 November 2014
Communicated by Dieter Jungnickel

MSC:
11T06
11T71
12E05

Keywords:
Irreducible polynomial
Primitive polynomial
Trace

ABSTRACT

We give a new proof of Fitzgerald's criterion for primitive polynomials over a finite field. Existing proofs essentially use the theory of linear recurrences over finite fields. Here, we give a much shorter and self-contained proof which does not use the theory of linear recurrences.

1. Introduction

Fitzgerald [1] gave a criterion for distinguishing primitive polynomials among irreducible ones by counting the number of nonzero coefficients in a certain quotient of polynomials. This characterization was then used to compute the minimum weight of certain binary BCH codes. Subsequently, Laohakosol and Pintoptang [2] modified and

E-mail address: samrith@gmail.com.

http://dx.doi.org/10.1016/j.ffa.2014.09.006
1071-5797/

extended the result of Fitzgerald using similar techniques and appealing to the theory of linear recurrences. Here, we prove Fitzgerald's original result by a more direct approach using elementary properties of the trace map.

2. Fitzgerald's theorem

In the following theorem, the condition $P(1) \neq 0$ is imposed to rule out the polynomial $P(x) = x + 1$ which is primitive in $\mathbb{F}_2[x]$.

Theorem 2.1 *(Fitzgerald). Let $P(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree k with $P(1) \neq 0$. Let $m = q^k - 1$ and define $g(x) = \frac{(x^m-1)}{(x-1)P(x)}$. Then $P(x)$ is primitive if and only if $g(x)$ is a polynomial with exactly $(q-1)q^{k-1} - 1$ nonzero terms.*

Proof. Let $P(x)$ be as in the hypothesis of the theorem. If $P(0) = 0$ then $P(x)$ cannot be primitive. So suppose $P(0) \neq 0$. Then $g(x)$ is necessarily a polynomial of degree at most $m - 1$. Let $Q(x)$ be the monic reciprocal of $P(x)$ and let $Q(x) = (x - \alpha_1) \cdots (x - \alpha_k)$ be the factorization of $Q(x)$ in $\mathbb{F}_{q^k}[x]$. Then

$$P(x) = a \prod_{i=1}^{k} (1 - \alpha_i x)$$

for some $a \in \mathbb{F}_q^*$. We then have the partial fraction decomposition

$$\frac{1}{P(x)} = \frac{1}{a} \sum_{i=1}^{k} \frac{a_i}{1 - \alpha_i x},$$

where $a_i = \alpha_i^{k-1}/Q'(\alpha_i)$ for $1 \leq i \leq k$. Expanding each term of the partial fraction formally as a power series and collecting terms, we obtain

$$\frac{1}{P(x)} = \frac{1}{a}\left(s_{k-1} + s_k x + s_{k+1} x^2 + \cdots\right),$$

where

$$s_r = \sum_{i=1}^{k} \frac{\alpha_i^r}{Q'(\alpha_i)} = \operatorname{Tr}\left(\frac{\alpha^r}{Q'(\alpha)}\right)$$

for each integer r and $\alpha = \alpha_1$. Here $\operatorname{Tr} : \mathbb{F}_{q^k} \to \mathbb{F}_q$ is the trace map. Now, we have

$$g(x) = \frac{x^m - 1}{(x-1)P(x)} = \frac{1}{a}\left(1 + x + \cdots + x^{m-1}\right)\left(s_{k-1} + s_k x + s_{k+1} x^2 + \cdots\right).$$