International Journal of Pure and Applied Mathematics
Volume 115 No. 3 2017, 529-532
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v115i3.6

ijpam.eu

A NOTE ON CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS WITH CHARACTERISTIC 2

Murat Alan[1] §, Betül Duman[2]
[1,2]Mathematics Department
Faculty of Arts and Sciences
Yildiz Technical University
Davutpasa Campus, 34210, Esenler, Istanbul, TURKEY

Abstract: Let $f(x)$ be an irreducible polynomial of degree m over the finite field $\mathbb{F}_q$ where q is a power of 2. We show that the polynomial $x^{2m} f\left(\frac{x^4+x^3+x+1}{x^2}\right)$ is an irreducible polynomial of degree $4m$ over $\mathbb{F}_q$ under some conditions on coefficients of $f(x)$.

AMS Subject Classification: 11C08, 12E05, 12E20
Key Words: finite fields, irreducible polynomials, composition of polynomials

1. Introduction

Irreducible polynomials over finite fields are of interest both for their own theoretical importance and for their applications on various areas of research including cryptography, coding theory or linear recurring sequences. One of the main tool to construct a new irreducible polynomial over a finite field from a given irreducible polynomial $P(x)$ with degree n is the composition of polynomials of the form $(g(x))^n P(f(x)/g(x))$. There are many results based on irreducibility of composition of polynomials over any finite fields, for example see [5], [2]. In

Received: March 10, 2017
Revised: May 30, 2017
Published: July 27, 2017

§Correspondence author

this note, by using the basic facts for construction of irreducible polynomials we propose a new member of composition of polynomials to produce an irreducible polynomial from a given irreducible polynomial over finite fields with characteristic 2.

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements of characteristic p, where p is a prime, and let $f(x) = a_0 + \ldots + a_{m-1}x^{m-1} + x^m \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m. For any $\alpha \in \mathbb{F}_{q^m}$ the *trace* $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ is defined by

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

If α is a root of $f(x)$ then $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -a_{m-1}$. For any polynomial $f(x)$ over $\mathbb{F}_q$ whose constant term is nonzero, the *reciprocal* of $f(x)$ is a polynomial $f^{\square}(x) = x^m f(\frac{1}{x})$ of degree m over $\mathbb{F}_q$ and the roots of $f^{\square}(x)$ are the reciprocals of the roots of $f(x)$. For more information on terminology and notations we refer [3], [4].

2. Main Theorem

The aim of this note is to give a proof of the following theorem.

Theorem 1 (Main Theorem)**.** *Let $f(x) = a_0 + \ldots + a_{m-1}x^{m-1} + x^m \in \mathbb{F}_q[x]$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree m where $q = 2^n$. Assume that $Tr_{\mathbb{F}_q/\mathbb{F}_2}(a_{m-1}) \neq 0$ and $Tr_{\mathbb{F}_q/\mathbb{F}_2}(a_1/a_0) \neq 0$. Then*

$$P(x) = x^{2m} f\left(\frac{x^4 + x^3 + x + 1}{x^2}\right)$$

is an irreducible polynomial over $\mathbb{F}_q$ of degree $4m$.

The proof of the theorem is based on a combination of the following results. The following theorem is essential for our study and it can be found in [1] too.

Theorem 2 (see [4], Theorem 3.7)**.** *Let $f(x), g(x) \in \mathbb{F}_q[x]$, and let $P(x) \in \mathbb{F}_q[x]$ be irreducible of degree n. Then $P(f/g) = g^n(x)P(f(x)/g(x))$ is irreducible over F_q if and only if $f(x) - \lambda g(x)$ is irreducible over $\mathbb{F}_{q^n}$ for some root $\lambda \in \mathbb{F}_{q^n}$ of $P(x)$.*

Theorem 3 (see [4], Theorem 3.5)**.** *The trinomial $x^p - x - b$, $b \in \mathbb{F}_q$ where q is a prime power p^m, is irreducible over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$.*

Theorem 4 (see [4], Theorem 3.10)**.** *Let $q = 2^m$ and let $P(x) = c_0 + \ldots + c_n x^n \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ of degree n. Then*

(i) $x^n P(x + x^{-1})$ *is irreducible over* $\mathbb{F}_q$ *if and only if* $Tr_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0) \neq 0$.

(ii) $x^n P^{\square}(x + x^{-1})$ *is irreducible over* $\mathbb{F}_q$ *if and only if* $Tr_{\mathbb{F}_q/\mathbb{F}_2}(c_{n-1}/c_n) \neq 0$.

Proof of The Main Theorem. Let α be a root of $f(x) = 0$ such that $\alpha \in \mathbb{F}_{q^m}$. Then

$$\begin{aligned} Tr_{\mathbb{F}_{q^m}/\mathbb{F}_2}(\alpha) &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)) \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(-a_{m-1}) \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(a_{m-1}) \neq 0. \end{aligned}$$

Then by Theorem 3, $g(x) = x^2 - x - \alpha$ is an irreducible trinomial over $\mathbb{F}_{q^m}$. Now consider the polynomial $h(x) = x^2 g(x + \frac{1}{x}) \in \mathbb{F}_{q^m}[x]$. By Theorem 4, $h(x)$ is irreducible over $\mathbb{F}_{q^m}$ if and only if $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_2}(\frac{-1}{-\alpha}) \neq 0$. Since the reciprocal of an irreducible polynomial is also irreducible, $(\frac{1}{a_0}) f^{\square}(x) = (\frac{1}{a_0}) x^m f(\frac{1}{x}) = (\frac{1}{a_0})(1 + a_{m-1}x + \ldots + a_1 x^{m-1} + a_0 x^m) \in \mathbb{F}_q[x]$ is the minimal polynomial of α^{-1} over $\mathbb{F}_q$. So

$$\begin{aligned} Tr_{\mathbb{F}_{q^m}/\mathbb{F}_2}\left(\frac{-1}{-\alpha}\right) &= Tr_{\mathbb{F}_{q^m}/\mathbb{F}_2}(\alpha^{-1}) \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})) \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(-\frac{a_1}{a_0}) \\ &= Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{a_1}{a_0}) \neq 0. \end{aligned}$$

Hence $h(x) = x^2 g(x + \frac{1}{x})$ is an irreducible polynomial over $\mathbb{F}_{q^m}$. So we have that

$$\begin{aligned} h(x) &= x^2 \left[\left(\frac{x^2+1}{x} \right)^2 + \left(\frac{x^2+1}{x} \right) + \alpha \right] \\ &= x^4 + x^3 + \alpha x^2 + x + 1 \end{aligned}$$

is an irreducible polynomial over $\mathbb{F}_{q^m}$. Then by Theorem 2, the composition $x^{2m} f\left(\frac{x^4+x^3+x+1}{x^2}\right)$ is an irreducible polynomial over $\mathbb{F}_q$ with degree $4m$. □

Corollary 5. *Let* $f(x) = 1 + x + a_2 x^2 + \ldots + a_{m-2} x^{m-2} + x^{m-1} + x^m$ *be a monic irreducible polynomial over* $\mathbb{F}_q$ *of degree* m *where* q *is an odd power of 2. Then* $P(x) = x^{2m} f(\frac{x^4+x^3+x+1}{x^2})$ *is an irreducible polynomial over* $\mathbb{F}_q$ *of degree* $4m$. *In particular* $P(x) = x^{2m} f(\frac{x^4+x^3+x+1}{x^2})$ *is an irreducible polynomial*

over $\mathbb{F}_2$ *of degree* $4m$ *if* $f(x) = 1 + x + a_2x^2 + \ldots + a_{m-2}x^{m-2} + x^{m-1} + x^m$ *is an irreducible polynomial over* $\mathbb{F}_2$ *of degree* m.

Example 6. (a) $f(x) = x^4 + x^3 + x^2 + x + 1$ is an irreducible polynomial over $\mathbb{F}_2$ $(\mathbb{F}_8)$. Then according the Corollary 5,

$$\begin{aligned} P(x) &= x^8 f\left(\frac{x^4 + x^3 + x + 1}{x^2}\right) \\ &= x^{16} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

is also an irreducible polynomial over $\mathbb{F}_2$ $(\mathbb{F}_8)$.

(b) Let $\mathbb{F}_8 = \mathbb{F}_2(\omega)$ where ω is a root of irreducible polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$. Then $f(x) = x^2 + (\omega^2 + 1)x + \omega + 1$ is an irreducible polynomial over $\mathbb{F}_8$ and $Tr_{\mathbb{F}_8/\mathbb{F}_2}(\omega^2 + 1) = Tr_{\mathbb{F}_8/\mathbb{F}_2}(\omega^2) + Tr_{\mathbb{F}_8/\mathbb{F}_2}(1) = 1 \neq 0$ and $Tr_{\mathbb{F}_8/\mathbb{F}_2}\left(\frac{\omega^2+1}{\omega+1}\right) = Tr_{\mathbb{F}_8/\mathbb{F}_2}(\omega + 1) = 1 \neq 0$. Since the conditions in the main theorem are satisfied, we conclude that

$$\begin{aligned} P(x) &= x^4 f\left(\frac{x^4 + x^3 + x + 1}{x^2}\right) \\ &= x^8 + \omega^2 x^6 + (\omega^2 + 1)x^5 + (\omega + 1)x^4 + (\omega^2 + 1)x^3 + \omega^2 x^2 + 1 \end{aligned}$$

is an irreducible polynomial over $\mathbb{F}_8$.

References

[1] S.D. Cohen, On irreducible polynomials of certain types in finite fields, *Proc. Cambridge Philos. Soc.*, **66** (1969), 335-344, **doi:** 10.1017/S0305004100045023.

[2] Melsik K. Kyureghyan, Gohar M. Kyureghyan, Irreducible compositions of polynomials over finite fields, *Designs, Codes and Cryptography*, **61**, No. 3 (2011), 301-314, **doi:** 10.1007/s10623-010-9478-5.

[3] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1987, **doi:** 10.1017/CBO9780511525926.

[4] A. Menezez, I. Blake, X. Gao, R. Mullin, S. Vanstone, T. Yaghoobian, *Application of Finite Fields*, Kluwer Academic Publishers, Boston, 1993, **doi:** 10.1007/978-1-4757-2226-0.

[5] Omran Ahmadi, Generalization of a theorem of Carlitz, *Finite Fields and Their Applications*, **17**, No. 5 (2011), 473-480, **doi:** 10.1016/j.ffa.2011.02.009.