Mathematical Problems of Computer Science 35, 99 103, 2011.

Irreducibility of Some Composite Polynomials Over Finite Fields *

Sergey Abrahamyan and Edita Harutyunyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail serj.abrahamyan@gmail.com, edita@ipia.sci.am

Abstract

Given the field $\mathcal{F}$ with q elements and of characteristics p and an irreducible polynomial $P(x) = c_n x^n + c_{n-1}x^{n-1+c_1x^n\cdots c_0}$ over $\mathcal{F}$. We prove that the composite polynomial $(dx^p - dx)^n\, p\left(\frac{ax^p-ax+c}{dx^p-dx}\right)$ is irreducible over $\mathcal{F}$ under certain conditions. Also a recursive construction of sequences of irreducible polynomials of degree $n2^k (k = 1, 2, 3, \cdots)$ over $\mathcal{F}_2$, is given.

1. Introduction

The subject of constructing irreducible polynomials over a finite field has been of considerable interest in recent years. Interest to it steams both from mathematical theory and practical applications At mathematical aspect, determining the irreducibility of a polynomial is an issue of interest in number theory, computer algebra, computational mathematics, theory of finite fields. At the practical aspect, it still remains an active subject, highly motivated by the fast development of coding theory and the appearance of cryptosystems in which implementation of finite fields fields arithmetic is required [3], [8].

There are known different composition and recursive construction techniques to generate irreducible polynomials over finite fields, among which polynomial composition method is considered to be most efficient.

The work concerns the questions of irreducibility of a polynomial composition over a finite field, more precisely we are interested in the following problem: given the field $\mathcal{F}$ with q elements and of characteristics p. Let ax^p-ax+c and dx^p-dx be relatively prime polynomials in $\mathcal{F}_q[x]$ and $P(x) = c_n x^n + c_{n-1}x^{n-1+r_1x^n\cdots r_0}$ be an irreducible polynomial over $\mathcal{F}$. Our aim is to determine irreducibility of the composite polynomial $(dx^p - dx)^n\, p\left(\frac{ax^p-ax+c}{dx^p-dx}\right)$ over $\mathcal{F}_{\mathrm{II}}$.

A number of interesting irreducibility results for composition of polynomials appear in the literature, including Varshamov [9], Kyuregyan [4]-[7], Cohen [2], [1] and perhaps the most important result for the present study is the following one due to Cohen.

Theorem 1:[Cohen [2]] *Let $f(x), g(x) \in \mathcal{F}_q[x]$ be relatively prime polynomials and let $P(x) \in \mathcal{F}_q[x]$ be an irreducible polynomial of degree n. Then the composition*

$$F(x) = g^n(x)P(f(x)/g(x))$$

*The work was supported by Armenian Target Programm 04.10.31.

is irreducible over $\mathcal{F}_q$ if and only if $f(x)-\alpha g(x)$ is irreducible over $\mathcal{F}_{q^n}$ for some root $\alpha \in \mathcal{F}_{q^n}$ of $P(x)$.

Some generalizations of polynomial composition results were derived by Kyuregyan [7], who considered several constructions which yields families of higher degree irreducible polynomials over finite fields starting from an irreducible polynomial.

2. Preliminaries

In this section we introduce some definitions and provide some auxiliary results that will be helpful to derive our main result.

Let $\mathcal{F}_{q^n}$ be a finite extension field over finite field $\mathcal{F}$. We state the following definitions.

Definition 1: *For $\alpha \in \mathcal{F}_{q^n}$ the trace $Tr_{\mathcal{F}_{q^n}|\mathcal{F}}(\alpha)$ of α over $\mathcal{F}$ is defined by*

$$Tr_{\mathcal{F}_{q^n}|\mathcal{F}}(\alpha) = \alpha + \alpha^q + \cdots \alpha^{q^{n-2}} + \alpha^{q^{n-1}}$$

Definition 2: *For $\alpha \in \mathcal{F}_{q^n}$ the norm $N_{\mathcal{F}_{q^n}|\mathcal{F}}$ of α over $\mathcal{F}$ is defined by*

$$N_{\mathcal{F}_{q^n}|\mathcal{F}}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \alpha^{q^{n-2}} \cdot \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$$

For convince we denote $Tr_{\mathcal{F}_{q^n}|\mathcal{F}} = Tr_{q^n|q}$ and $N_{\mathcal{F}_{q^n}|\mathcal{F}} = N_{q^n|q}$.

The following results address to our question.

Proposition 1:[[3], Theorem 3.78] *Let $\alpha \in \mathcal{F}$ and let p be the characteristic of $\mathcal{F}$. Then the trinomial $x^p - x - \alpha$ is irreducible in $\mathcal{F}[x]$ if and only if it has no root in $\mathcal{F}$.*

Proposition 2: [[3], Corollary 3.79] *With the notation of the proposition above, the trinomial $x^p - x - \alpha$ is irreducible in $\mathcal{F}[x]$ if and only if $Tr_{\mathcal{F}}(\alpha) \neq 0$.*

Recall that for a polynomial $F(x)$ of degree n its monic reciprocal is defined by

$$F^*(x) = \frac{1}{F(0)} x^n F(1/x).$$

3. Irreducibility of Polynomial Compositions

In this section we shall establish the irreducibility of the composite polynomial $(dx^p - dx)^n p\left(\frac{ax^p-ax+c}{dx^p-dx}\right)$ over $\mathcal{F}_q$.

Theorem 2: *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree $n \geq 1$ over $\mathcal{F}$ and $ax^p - ax + c$ and $dx^p - dx$ be relatively prime polynomials in $\mathcal{F}_q[x]$, $a, b \in \mathcal{F}$. Then*

$$F(x) = (dx^p - dx)^n P\left(\frac{ax^p - ax + c}{dx^p - dx}\right)$$

is an irreducible polynomial of degree pn over $\mathcal{F}$ if and only if

$$Tr_{q|p}\left(\frac{cd_1}{d_0}\right) \neq 0.$$

where $d_1 = \frac{1}{d}\sum_{i=1}^{n} i\, c_i \left(\frac{a}{d}\right)^{i-1} = \frac{1}{d}P'\left(\frac{a}{d}\right)$ and $d_0 = \sum_{i=0}^{n} c_i \left(\frac{a}{d}\right)^i = P\left(\frac{a}{d}\right)$.

Proof: By Theorem 2 the polynomial $F(x)$ is irreducible over $\mathcal{F}$ if and only if $(a-d\alpha)x^p-(a-d\alpha)x+c$ is irreducible over $\mathcal{F}_{q^n}$, where $\alpha \in \mathcal{F}_{q^n}$ is a root of $P(x)$. And by Proposition 2 $(a-d\alpha)\left(x^p-x-\frac{c}{(d\alpha-a)}\right)$ is irreducible over $\mathcal{F}_{q^n}$ if and only if $Tr_{q^n|p}\left(\frac{c}{d\alpha-a}\right)\neq 0$.

From the properties of trace we will have

$$Tr_{q^n|p}\left(\frac{c}{d\alpha-a}\right)=Tr_{q|p}\left(c\cdot Tr_{q^n|q}\frac{1}{d\alpha-a}\right).$$

Compute the trace

$$Tr_{q^n|q}\left(\frac{1}{d\alpha-a}\right).$$

We denote $P\left(\frac{x+a}{d}\right)$ as follows:

$$P\left(\frac{x+a}{d}\right)=\sum_{i=0}^{n}c_i\left(\frac{x+a}{d}\right)^i=\sum_{i=0}^{n}d_ix^i=D(x).$$

Since α is a root of $P(x)$ then $d\alpha-a$ must be a root of $D(x)=P\left(\frac{x+a}{d}\right)$ and therefore $\frac{1}{d\alpha-a}$ is a root of $D^*(x)$ (recall here that $D^*(x)$ is a reciprocal polynomial of $D(x)$). Then

$$Tr_{q^n|q}\left(\frac{1}{d\alpha-a}\right)=\frac{d_1}{d_0}.$$

Next we compute d_1 and d_0

$$d_0 = D(0)=\sum_{i=0}^{n}c_i\left(\frac{a}{d}\right)^i=P\left(\frac{a}{d}\right)$$

$$d_1 = D'(0)=P'\left(\frac{x+a}{d}\right)\Big|_{x=0}=\frac{1}{d}\sum_{i=0}^{n}i\,c_i\left(\frac{a}{d}\right)^{i-1}=\frac{1}{d}P'\left(\frac{a}{d}\right).$$

Thus

$$Tr_{q^n|q}\left(\frac{1}{d\alpha-a}\right)=\frac{d_1}{d_0}$$

and

$$Tr_{q^n|p}\left(\frac{c}{d\alpha-a}\right)=Tr_{q^n|p}\left(\frac{d_1}{d_0}\right).$$

The proof of the theorem is completed.

A corollary below describes a particular case of Theorem 2 with $q=2^s$.

Corollary 1: *Let $P(x)=\sum_{i=0}^{n}c_ix^i$ be an irreducible polynomial of degree $n\geq 1$ over $\mathcal{F}_{2^s}$. Then*

$$F(x)=\left(x^2-x\right)^nP\left(\frac{x^2-x+1}{x^2-x}\right)$$

is irreducible over $\mathcal{F}_{2^s}$ if and only if

$$Tr_{2^s|2}\left(\frac{P'(1)}{P(1)}-n\right)\neq 0.$$

As an application of Theorem 2 we study the following example.

Example: Consider the Galois field $\mathcal{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$, where α is a root of the irreducible polynomial x^2+x+2 over $\mathcal{F}_3$. Given an irreducible polynomial $P(x) = x^2+(\alpha+1)x+2\alpha$ over $\mathcal{F}_9$ and $f(x) = \alpha x^3 - \alpha x + 2$ and $g(x) = (\alpha+1)x^3 - (\alpha+1)x$. Then

$$\begin{aligned} F(x) &= \left((\alpha+1)x^3-(\alpha+1)x\right)^2 P\left(\frac{\alpha x^3-\alpha x+2}{(\alpha+1)x^3-(\alpha+1)x}\right) \\ &= (\alpha x^3-\alpha x+2)^2 + (\alpha+1)(\alpha x^3-\alpha x+2)\left((\alpha+1)x^3-(\alpha+1)x\right) \\ &+2\alpha\left((\alpha+1)x^3-(\alpha+1)x\right)^2 \\ &= 2\alpha x^6 + x^6 + 2\alpha x^4 + x^4 + 2\alpha x^2 + x^2 + \alpha x^3 - \alpha x^3 - \alpha x + 1 + \alpha x^6 \\ &+x^6 + \alpha x^4 + x^4 + 2\alpha x^3 + x^3 + \alpha x^2 + x^2 - 2\alpha x - x + 2\alpha x^6 \\ &+2x^6 + 2\alpha x^4 + 2\alpha x^2 + 2x^2 + 2x^4 \\ &= (2\alpha+1)x^6 + (2\alpha+1)x^4 + x^3 + (2\alpha+1)x^2 + 2x + 1 \end{aligned}$$

is an irreducible polynomial over $\mathcal{F}_3$ by Theorem 2.

4. Recursive Construction

In this section we shall describe a recurrent method that allows constructions of families of irreducible polynomials over $\mathcal{F}_q$ by using above-given polynomial composition.

Theorem 3: *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree $n \geq 2$ over $\mathcal{F}_{2^s}$. Define*

$$\begin{aligned} F_0(x) &= P(x), \\ F_k(x) &= \left(x^2+x+1\right)^{t_{k-1}} \cdot F_{k-1}\left(\frac{x^2+x}{x^2+x+1}\right), \; k \geq 1 \end{aligned}$$

where $t_k = n2^k$ denotes the degree of $F_k(x)$. Then $F_k(x)$ is irreducible over $\mathcal{F}_{2^s}$ if and only if $Tr_{2^s|2}\left(\frac{p'(1)}{p(1)}+n\right) \neq 0$ and $Tr_{2^s|2}\left(\frac{c_1}{c_0}+n\right) \neq 0$.

5. Acknowledgment

This study was supported by the grant ('GRASP-10-05') of the National Academy of Sciences of RA. the National Foundation of Science and Advanced Technologies (RA) and Civilian Research and Development Foundation (US).

References

[1] S. E. Abrahamyan. "Construction of Irreducible Polynomials over Finite Fields". *Proceedings of 12th International Workshop, CASC 2010. in Lecture Notes in Computer Science.* vol. 6244. Gerdt. pp. 3-4. 2010.

[2] S. D. Cohen. "On irreducible polynomials of certain types in finite fields". *Proc. Cambridge Philos. Soc.*. vol. 66. pp. 335 344. 1969.

[3] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press. 1987.

[4] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $\mathcal{F}_q$ of odd characteristics". *Finite Fields Appl.*, vol. 9, pp. 39–58, 2003.

[5] M. K. Kyuregyan, "Iterated constructions of irreducible polynomials over finite fields with linearly independent roots". *Finite Fields , Appl.*, vol. 10, pp. 323-431, 2004.

[6] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $\mathcal{F}_q$ of odd characteristics II". *Finite Fields, Appl.*, vol. 12, pp. 357–378, 2006.

[7] M. K. Kyuregyan and G. M. Kyuregyan, "Irreducible Compositions of Polynomials over Finite Fields", *Design, Codes and Cryptography*, Available online: ISSN:0925-1022 2010.

[8] A. Menezes, I.F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian. *Applications of Finite Fields*. Kluwer Academic Publishers, Boston- Dordrecht- Lancaster, 1993.

[9] R. R. Varshamov, "A general method of synthesizing irreducible polynomials over Galois fields", *Soviet Math. Dokl.*, vol. 29, 334 – 336, 1984.

Որոշ բաղադրյալ բազմանդամների չբերվելիությունը վերջավոր դաշտերի վրա

Ս. Աբրահամյան և Է. Հարությունյան

Ամփոփում

Աշխատանքը նվիրված է վերջավոր դաշտերի վրա չբերվող բազմանդամների բաղադրությունների կառուցմանը: Տրված է q հզորությամբ, p բնութագրիչով $\mathcal{F}_q$ դաշտը և $\mathcal{F}_q$ դաշտի վրա $P(x) = c_n x^n + c_{n-1}x^{n-1+c_1}x^{n-\cdots c_0}$ չբերվող բազմանդամը: Ցույց է տրված, որ $(dx^p - dx)^n\, p\left(\frac{ax^p-ax+c}{dx^p-dx}\right)$ բաղադրությունը չբերվող է $\mathcal{F}_q$ դաշտի վրա որոշակի պայմանների դեպքում: Ավելին, տրված է $\mathcal{F}_{2^n}$ դաշտի վրա $n2^k (k = 1, 2, 3, \cdots)$ աստիճանի չբերվող բազմանդամների կառուցման հաջորդական եղանակ: