Mathematical Problems of Computer Science 35, 26 32, 2011.

Constructing Methods for Irreducible Polynomials

Mahmood Alizadeh

Islamic Azad University- Ahvaz Branch
E-mail: Alizadeh@iauahvaz.ac.ir

Abstract

In this paper we study the irreducibility of some composite polynomials, constructed with a polynomial composition method over finite fields. Furthermore, a recurrent method for constructing families of irreducible polynomials of higher degree from given irreducible polynomials over finite fields is given.

1. Introduction

In this century many mathematicians have been trying to study finite fields and to construct irreducible polynomials over finite fields. The problem of irreducibility of polynomials over galois fields is a case of special interest and plays an important role in modern engineering. One of the methods to construct irreducible polynomials is the polynomial composition method that allows constructions of irreducible polynomials of higher degree from given irreducible polynomials over finite fields.

Let F_q be the Galois field of order $q = p^s$, where p is a prime and s is a natural number. Also suppose that $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over F_q of degree n. Some authors have been studying the irreducibility of the polynomial

$$F(x) = (dx^p - rx + h)^n P\left(\frac{ax^p - bx + c}{dx^p - rx + h}\right). \tag{1}$$

For some particular cases. Varshamov studied one case from (1) and gave the following proposition:

Proposition 1: ([11], Theorem 3.13). *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over F_q and p be the characteristic of F_q. Then the polynomial $P(x^p - x - \delta_0)$ is irreducible over F_q if and only if*

$$Tr_{q|p}(n\delta_0 - c_{n-1}) \neq 0.$$

Also, for this case, Kyuregyan gave a recurrent method for constructing irreducible polynomials in the following proposition:

Proposition 2: (Kyuregyan [10], Theorem 2). *Let $F(x) = \sum_{u=0}^{n} c_u x^u$ be an irreducible polynomial over F_q and suppose that there exists an element $\delta_0 \in F_p$ such that $F(\delta_0) = a$, with $a \in F_p^*$ and*

$$Tr_{q|p}(n\delta_0 - c_{n-1}) Tr_{q|p}(F'(\delta_0)) \neq 0.$$

Let $g_0(x) = x^p - x + \delta_0$ *and* $g_k(x) = x^p - x + \delta_k$ *. where* $\delta_k \in F_p^*$ *.* $k \geq 1$ *. Define* $F_0(x) = F(g_0(x))$ *, and* $F_k(x) = F_{k-1}^*(g_k(x))$ *for* $k \geq 1$ *, where* $F_{k-1}^*(x)$ *is the reciprocal polynomial of* $F_{k-1}(x)$*. Then for each* $k \geq 0$*. The Polynomial* $F_k(x)$ *is irreducible over* F_q *of degree* $n_k = n.p^{k+1}$*.*

We note that the above Proposition is the Generalization of Varshamov's theorem. that the reader can find in ([11], theorem 3.19). He also gave another recurrent method for constructing irreducible polynomials in the following proposition:

Proposition 3: (Kuyregyan [9], corollary 2). *Let s be odd integer,* δ *be any element of* $F_{2^s}^*$*, and the sequence of functions* $\varphi_m(x)$ *be defined by*

$$\varphi_m(x) = a_m(x) + \delta b_m(x)$$

under the initial condition

$$\varphi_0(x) = x + \delta.$$

Then the polynomial $\varphi_m(x)$ of degree $2m$ defined by the recurrent relation

$$\varphi_m(x) = x^{2^{m-1}} \varphi_{m-1}(x + \frac{\delta^2}{x})$$

is irreducible over F_{2^s} , where

$$a_1(x) = x^2 + \delta^2 \quad , \quad b_1(x) = x,$$

$$a_m(x) = a_{m-1}^2(x) + b_{m-1}^2(x)$$

and also

$$b_m(x) = a_{m-1}(x) b_{m-1}(x).$$

But Cohen studied another case from (1), when q is odd. He also gave a recurrent method for constructing irreducible polynomials in the following Proposition:

Proposition 4: (Cohen [6]). *Let* q *be odd, and* $f_0(x) \in F_q[x]$ *be a monic irreducible polynomial of degree* n *, where* n *is even when* $q \equiv 3(mod4)$ *such that* $f_0(1)f_0(-1)$ *is a non-square in* F_q*. Then for* $r \geq 1$

$$f_r(x) = (2x)^n f_{r-1}(\frac{x^2+1}{x})$$

is irreducible of degree $2^r n$*.*

The aim of this paper is to determine under what conditions

$$F(x) = (x^p - x + \delta_1)^n P(\frac{x^p - x + \delta_0}{x^p - x + \delta_1})$$

is irreducible over F_q,where $P(x)$ is an irreducible polynomial of degree n over F_q. and also to give a recurrent method for constructing families of irreducible polynomials $F_k(x)$. for $k \geq 0$ over the finite fields. when $F_0(x) = P(x)$.Such polynomials are used to implement arithmetic in extension fields and are found in many applications. including coding theory [1. 8] cryptography[2. 4. 7], computer algebra system [3].

2. Irreducibility of Composition Polynomials

Definition 1: *Let F_{q^n} be a finite extension field of the finite field F_q .For $\alpha \in F_{q^n}$, the trace $Tr_{q^n|q}(\alpha)$ over F_q is defined by*

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}.$$

Proposition 5: ([11].theorem 3.5) *The trinomial $x^p - x - b$, $b \in F_q$ where q is a prime power p^m , is irreducible over F_q if and only if*

$$Tr_{q|p}(b) \neq 0.$$

Let $f(x). g(x) \in F_q[x]$ and let $P(x) = \sum_{i=0}^{n} c_i x^i \in F_q[x]$ of degree n. Then the following composition

$$F(x) = g^n(x) P(\frac{f(x)}{g(x)}) = \sum_{i=0}^{n} c_i f^i(x) g^{n-i}(x)$$

is again a polynomial in $F_q[x]$. The problem is to determine under what conditions $F(x)$ is irreducible over F_q. Obviously. for $F(x)$ to be irreducible, $P(x)$ must be irreducible and $g(x)$ and $f(x)$ to be relatively prime.

Proposition 6: (Cohen [5]). *Let $f(x), g(x) \in F_q[x]$ with $gcd(f(x). g(x)) = 1$, and let $P(x) \in F_q[x]$ be an irreducible polynomial of degree n. Then*

$$F(x) = g^n(x) P(\frac{f(x)}{g(x)})$$

is irreducible over F_q if and only if $f(x) - \alpha g(x)$ is irreducible over F_{q^n}, for some root $\alpha \in F_{q^n}$ of $P(x)$.

Theorem 1: *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be irreducible over F_q of degree n and let $\delta_0, \delta_1 \in F_q$, $\delta_0 \neq \delta_1$. then*

$$F(x) = (x^p - x + \delta_1)^n P(\frac{x^p - x + \delta_0}{x^p - x + \delta_1})$$

is irreducible polynomial of degree pn over F_q if and only if

$$Tr_{q|p}((\delta_0 - \delta_1)\frac{P'(1)}{P(1)} - n\delta_1) \neq 0.$$

Proof: Proposition 6 implies that $F(x)$ is an irreducible polynomial over F_q if and only if

$$x^p - x - (\frac{\delta_0 - \delta_1 \alpha}{\alpha - 1})$$

is irreducible over F_{q^n} . where α is a root of $P(x)$. Then by proposition 5. $P(x)$ is irreducible over F_q if and only if

$$Tr_{q^n|p}(\frac{\delta_0 - \delta_1 \alpha}{\alpha - 1}) \neq 0.$$

But

$$Tr_{q^n|p}(\frac{\delta_0 - \delta_1 \alpha}{\alpha - 1}) = Tr_{q|p}(Tr_{q^n|q}(\frac{\delta_0 - \delta_1 \alpha}{\alpha - 1})). \quad (2)$$

Also

$$Tr_{q^n|q}(\frac{\delta_0-\delta_1\alpha}{\alpha-1}) = Tr_{q^n|q}(\frac{\delta_0}{\alpha-1}) - Tr_{q^n|q}(\frac{\delta_1\alpha-\delta_1+\delta_1}{\alpha-1}) = Tr_{q^n|q}(\frac{\delta_0}{\alpha-1}) - Tr_{q^n|q}(\delta_1+\frac{\delta_1}{\alpha-1})$$

$$= \delta_0 Tr_{q^n|q}(\frac{1}{\alpha-1}) - (\delta_1 Tr_{q^n|q}(1) + \delta_1 Tr_{q^n|q}(\frac{1}{\alpha-1})) = (\delta_0-\delta_1)Tr_{q^n|q}(\frac{1}{\alpha-1}) - n\delta_1. \quad (3)$$

Now since α is a root of $P(x)$. $\alpha-1$ is a root of $P(x+1)$ and $\frac{1}{\alpha-1}$ is a root of $P^*(x+1)$ and also

$$P(x+1) = \sum_{i=0}^{n} c_i(x+1)^i = \sum_{i=0}^{n} d_i x^i. \quad (4)$$

where $d_i \in F_q$ are coefficients of $P(x+1)$. for every $0 \leq i \leq n$. So

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

Now, substituting zero for x in (4) implies that

$$d_0 = \sum_{i=0}^{n} c_i = P(1).$$

and substituting zero for x in

$$P'(x+1) = \sum_{i=0}^{n} ic_i(x+1)^{i-1}$$

implies that

$$d_1 = \sum_{i=0}^{n} ic_i = P'(1).$$

Therefore

$$Tr_{q^n|q}(\frac{1}{\alpha-1}) = \frac{P'(1)}{P(1)}. \quad (5)$$

Then by(2),(3),(5)

$$Tr_{q^n|p}(\frac{\delta_0-\delta_1\alpha}{\alpha-1}) = Tr_{q|p}((\delta_0-\delta_1)\frac{P'(1)}{P(1)} - n\delta_1)).$$

At the end of proof. we note that $P(1)$ is not zero, because $P^*(x+1)$ is irreducible over F_q and $P(1)$ is its constant term.

The theorem is proved.

Example: Consider the Galois field $F_9 = \{0.1, 2. \alpha. \alpha+1. \alpha+2. 2\alpha. 2\alpha+1, 2\alpha+2\}$ where α is a root of the irreducible polynomial x^2+x+2 over F_3 . $P(x) = x^2+(\alpha+1)x+2\alpha$ is an irreducible polynomial over F_9 .Let $f(x) = x^3-x+(\alpha+2)$ and $g(x) = x^3-x+2\alpha$. So by Theorem 1

$$F(x) = (x^3-x+2\alpha)^2 P(\frac{x^3-x+(\alpha+2)}{x^3-x+2\alpha})$$
$$= (x^3-x+(\alpha+2))^2 + (\alpha+1)(x^3-x+(\alpha+2))(x^3-x+2\alpha)$$
$$+2\alpha(x^3-x+2\alpha)^2$$

$$= x^6 + x^4 + (2\alpha+1)x^3 + x^2 + (\alpha+2)x + 2$$
$$+(\alpha+1)x^6+(\alpha+1)x^4+(2\alpha+2)x^3+(\alpha+1)x^2-(2\alpha+2)x+(\alpha+1)$$
$$+2\alpha x^6 - \alpha x^4 + (\alpha+2)x^3 + 2\alpha x^2 + (2\alpha+1)x + (2\alpha+1)$$
$$= 2x^6 + 2x^4 + 2(\alpha+1)x^3 + 2x^2 + (\alpha+1)x + 1$$

is an irreducible polynomial over F_9.

Corollary 1: *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be irreducible over F_p of degree n and let $\delta_0, \delta_1 \in F_p$, $\delta_0 \neq \delta_1$. then*

$$F(x) = (x^p - x + \delta_1)^n P(\frac{x^p - x + \delta_0}{x^p - x + \delta_1})$$

is irreducible polynomial of degree pn over F_p if and only if

$$(\delta_0 - \delta_1)P'(1) - nP(1) \neq 0$$

3. Recurrent Method

Theorem 2: *Let $F_0(x)$ be an irreducible polynomial of degree p over F_p .Also for $\delta \in F_p$,$\delta + 1 \neq 0$ and $\delta \neq 1$,$F_0'(\delta).F_0'(1) \neq 0$. Then for each $k \geq 1$*

$$F_k(x) = (x^p - x + 1)^{p^k} F_{k-1}(\frac{x^p - x + \delta}{x^p - x + 1})$$

is a sequence of irreducible polynomials over F_p of degree p^{k+1}.

Proof: By corollary 1 and hypotheses theorem, $F_1(x)$ is irreducible over F_p , of degree p^2.

Let for $k \geq 1$, $F_{k-1}(x) = \sum_{i=0}^{p^k} u_i x^i$.Then

$$F_k(x) = (x^p - x + 1)^{p^k} \sum_{i=0}^{p^k} u_i (\frac{x^p - x + \delta}{x^p - x + 1})^i$$

$$= \sum_{i=0}^{p^k} u_i (x^p - x + \delta)^i (x^p - x + 1)^{p^k - i}$$

$$= u_0 (x^p - x + 1)^{p^k} + \sum_{i=1}^{p^k - 1} u_i (x^p - x + \delta)^i (x^p - x + 1)^{p^k - i}$$
$$+ u_{p^k} (x^p - x + \delta)^{p^k}$$

So

$$F_k'(x) = \sum_{i=1}^{p^k-1} u_i [-i(x^p - x + \delta)^{i-1}(x^p - x + 1)^{p^k - i} - (x^p - x + 1)^{p^k - i - 1}(x^p - x + \delta)^i (p^k - i)]$$

$$= -\sum_{i=1}^{p^k-1} u_i [(x^p - x + \delta)^{i-1}(x^p - x + 1)^{p^k - i - 1}][i(x^p - x + 1) + (p^k - i)(x^p - x + \delta)]$$

$$= -\sum_{i=1}^{p^k-1} u_i [(x^p - x + \delta)^{i-1}(x^p - x + 1)^{p^k - i - 1}].[i(1 - \delta)].$$

Then

$$F'_k(x) = (\delta - 1)\sum_{i=1}^{p^k-1} iu_i[(x^p - x + \delta)^{i-1}.(x^p - x + 1)^{p^k-i-1}] \text{ for all } k \geq 1. \quad (6)$$

So

$$F'_k(1) = (\delta - 1)F'_{k-1}(\delta). \qquad \text{for } k \geq 1. \quad (7)$$

Also by (6) we have

$$F'_k(\delta) = F'_k(1), \qquad \text{for } k \geq 1. \quad (8)$$

So by (7)

$$F'_1(1) = (\delta - 1)F'_0(\delta) \neq 0.$$

Also by (8) $F'_1(\delta) \neq 0$, so $F'_1(\delta).F'_1(1) \neq 0$. Now let $F_{k-1}(x)$ be an irreducible polynomial of degree p^k and

$$F'_{k-1}(\delta).F'_{k-1}(1) \neq 0.$$

Then by (7) and (8) it is clear that

$$F'_k(\delta)F'_k(1) \neq 0$$

so proof is completed by induction on k .

Corollary 2: *Let $F_0(x) = x^p + \beta_0 x + \beta_1$ be an irreducible polynomial over F_p, and let $\delta \in F_p$, $\delta \neq 1$ and $\beta_0 \neq 0$. Then for each $k \geq 1$*

$$F_k(x) = (x^p - x + 1)^{p^k} F_{k-1}\left(\frac{x^p - x + \delta}{x^p - x + 1}\right)$$

is a sequence of irreducible polynomials over F_p of degree p^{k+1}.

References

[1] E.R. Berlekamp. Algebraic coding theory. Mc Graw-Hill, New York. 1968.

[2] I.F. Blake. G.Seroussi, N.P.Smart. *Elliptic curves in cryptography*. Cambridge University Press, Cambridge . reprinted 2000.

[3] J.Calment. "Algebraic algorithms in GF(q)", *Discrete Math.*. vol. 56. pp. 101-109. 1985.

[4] B.Chor. R.Rivest. "Aknapsack-type public key cryptosystem based on arithmetic in finite fields". *IEEE Trans. Inform. Theory*. vol. 34, pp. 901-909. 1988.

[5] S.D.Cohen. "On irreducible polynomials of certain types in finite fields". *Pros. Cambridge philos. Soc.* vol. 66. pp. 335-344. 1969.

[6] S.D.Cohen. "The explicit construction of irreducible polynomial over finite fields".*Des. Codes cryptogr.*. vol. 2. pp. 169-174. 1992.

[7] N.Koblitz. *Algebraic aspects of cryptography*, Springer. Berlin 1998.

[8] R. Lidl. H.Niederreiter. *Finite fields*. Cambridge University. Press Cambridge 1987.

[9] M. Kyuregyan. "Recurrent methods for constructing irreducible polynomials over $GF(2^s)$". *Finite fields and their applications.* vol. 8. pp. 52-68. 2002.

[10] M.K. Kyuregyan. "Iterated constructions of irreducible polynomials over finite fields with linearly independent roots". *Finite fields and their applications.* vol. 10. pp. 323-341. 2004.

[11] A.J. Menezes, I. F. Blake , X.Gao. R.C.Mullin. S.A.Vanstone. T.Yaghoobian. *Applications of finite fields.* Kluwer Academic publishers. Boston. 1993.

Չբերվող բազմանդամների կառուցման եղանակ

Մ. Ալիզադեհ

Ամփոփում

Այս աշխատանքում մենք ուսումնասիրում ենք որոշ կոմպոզիցիոն բազմանդամների չբերվելիությունը, որոնք կառուցված են բազմաքնդամային կոմպոզիցիոն մեթոդով, վերջավոր դաշտերի վրա: Ավելին տրվել է ռեկուրենտ մեթոդ, վերջավոր դաշտերի վրա տրված չբերվող բազմանդամից բարձր աստիճանի չբերվող բազմանդամ կառուցելու համար: