ONE METHOD FOR CONSTRUCTING IRREDUCIBLE POLYNOMIALS
OVER $F_q$ OF ODD CHARACTERISTICS

Knarik Kyuregyan
Institute for Informatics and Automation Problems
Yerevan, Armenia

ABSTRACT

In this paper a new method for construction of irreducible polynomial over finite fields of odd $p = 2^m + 1$ characteristics is presented, $m$ is a natural number.

Keywords: Irreducible polynomial, Minimal polynomial, Odd characteristic, Galois field

1. INTRODUCTION

The problem of presenting a fast, effective algorithm for constructing irreducible polynomials over the finite field is one of the challenging and important problems in computer algebra, coding theory, cryptography and theory of finite fields.

Let $F_q$ be the Galois field of order $q = p^s$, where $p = 2^m + 1$ is an odd prime, $s$ and $m$ are natural numbers. The aim of this paper is to present a new method for constructing irreducible polynomials over $F_q$. Of more relevance to our study are the Corollary 3.6[2] and the Theorem (Cohen) 3.7 in [2], where it was established under what conditions $F(x) = g^n(x)P(f(x)/g(x))$ is irreducible.

We formulate the result as Theorem 2.

2. CONSTRUCTING IRREDUCIBLE POLYNOMIALS

We consider especially the case, when the characteristic of Galois field is 3.

Theorem 1. Let $g^{(0)}(x) = \sum_{u=0}^{n} a_u^{(0)} x^u \in F_q[x]$ be the minimal polynomial of an element $\alpha \in F_q^n$ over $F_q$, i.e. the irreducible polynomial of degree $n > 1$, of order $e_0$ and with at least one coefficient $a_{2i+1}^{(0)} \neq 0 \left(0 \leq i \leq \left\lceil \frac{n}{2} \right\rceil \right)$. Then the polynomials of degree $n$

$$g^{(k)}(x) = (-1)^n \sum_{j=0}^{2j} \sum_{u=0}^{n} (-1)^u a_u^{(k-1)} a_{2j-u}^{(k-1)} x_j$$

where $a_u^{(k-1)}$ and $a_{2j-u}^{(k-1)}$ are coefficients of $g^{(k-1)}(x) = \sum_{u=0}^{n} a_u^{(k-1)} x^u$ minimal polynomial of an element $\alpha^{2k-1}$, is the minimal polynomial of $\alpha^{2^k}$ and is of the order $e_k = \frac{e_{k-1}}{\gcd(e_{k-1}, 2)}$ for every $k \geq 1$.

Proof. According to Theorem 8[1] (Proposition 3[3]), if $g^{(0)}(x)$ is the minimal polynomial of $\alpha$, then

$$g^{(1)}(x) = (-1)^n \sum_{j=0}^{2j} \sum_{u=0}^{n} (-1)^u a_u^{(0)} a_{2j-u}^{(0)} x^j$$

1 $\lfloor x \rfloor$ is the largest integer less than or equal to $x$ and $\lceil x \rceil$ is the smallest integer greater or equal to $x$. 
polynomial is the minimal polynomial of $\alpha^2$, therefore, it is irreducible polynomial. Moreover the $e_1$ order of $g^{(1)}(x)$ is equal to $\frac{e_0}{\gcd(e_0,2)}$.

As the coefficients of $g^{(1)}(x)$ are from $F_q$, we can write

$$g^{(1)}(x) = \sum_{u=0}^{n} a^{(1)}_u x^u \in F_q[x].$$

Based on a view of (1), especially on the coefficient $(-1)^u a^{(0)}_{u} a^{(0)}_{2j-u}$ of $x^j$, if at least one coefficient $a^{(0)}_{2j+1} \neq 0$ of $g^{(0)}(x)$, then we will have at least one coefficient $a^{(1)}_{2j+1} \neq 0$ of $g^{(1)}(x)$. And so implying the proof of Theorem 8[1] on the polynomial $g^{(1)}(x)$, we can show that

$$g^{(2)}(x) = (-1)^n \sum_{j=0}^{n-1} \sum_{u=0}^{2j} (-1)^u a^{(1)}_u a^{(1)}_{2j-u} x^j$$

is the minimal polynomial of $\alpha^4$ and of order $e_2 = \frac{e_1}{\gcd(e_1,2)}$.

With the same logic are constructed the minimal polynomials of $\alpha^{2k}$ for every $k \geq 3$.

**Theorem 2.** Let $g^{(0)}(x) = \sum_{u=0}^{n} a^{(0)}_u x^u \in F_q[x]$ be the minimal polynomial of an element $\alpha \in F_q^n$. $Tr_{q|p} \left( a^{(1)}_1/a^{(1)}_0 \right) \neq 0$, where $a^{(1)}_1$ and $a^{(0)}_0$ are coefficients of the minimal $g^{(1)}(x)$ polynomial of an element $\alpha^2 \in F_q^n$. Then

$$F(x) = x^n g^{(1)} \left( \frac{x^p-1}{x} \right)$$

polynomial is irreducible.

**Proof.** Using the irreducibility of polynomial $g^{(1)}(x)$ over $F_q$, we have the following relation over the field $F_q^n$

$$g^{(1)}(x) = \prod_{u=0}^{n-1} (x - \alpha^{2q^u}).$$

In the last relation substituting $\frac{x^p-1}{x}$ for $x$, we have

$$g^{(1)} \left( \frac{x^p-1}{x} \right) = \prod_{u=0}^{n-1} \left( \frac{x^p-1}{x} - \alpha^{2q^u} \right). \quad (2)$$

Multiplying the both sides of (2) by $x^n$, we have

$$x^n g^{(1)} \left( \frac{x^p-1}{x} \right) = x^n \prod_{u=0}^{n-1} \left( \frac{x^p-1}{x} - \alpha^{2q^u} \right),$$

and then making some trivial operations in the right-hand side, we obtain

$$F(x) = x^n g^{(1)} \left( \frac{x^p-1}{x} \right) = \prod_{u=0}^{n-1} \left( x^p - \alpha^{2q^u} x - 1 \right).$$

According to Theorem (Cohen) 3.7[2], $F(x)$ is irreducible over $F_q$ if and only if $x^p - \alpha^2 x - 1$ is irreducible over $F_q^n$. From the theorem requirement we have $Tr_{q|p} \left( a^{(1)}_1/a^{(1)}_0 \right) \neq 0$, hence

$$Tr_{q^n|p} \left( 1/\alpha^p \right) = \left( Tr_{q^n|p} \left( 1/\alpha \right) \right)^p = \left( Tr_{q|p} \left( Tr_{q^n|q} \left( 1/\alpha \right) \right) \right)^p = \left( Tr_{q|p} \left( a^{(1)}_1/a^{(1)}_0 \right) \right)^p \neq 0.$$
Thus, due to Corollary 3.6[2], \( x^p - \alpha^2 x - 1 \) is irreducible over \( F_q^n \), hence \( F(x) \) is irreducible. With the same analogy we can construct

\[
F(x) = x^n g^{(1)} \left( \frac{x^p - 1}{x} \right)
\]

irreducible polynomial over \( F_q \) for any prime \( p = 2^m + 1 \) and \( q = p^s \), where \( s \) and \( m \) are natural numbers and \( g^{(1)}(x) \) is the minimal polynomial of \( \alpha^{2^{m+1}} \).

3. CONCLUSION

In this paper we are constructing

\[
F(x) = x^n g^{(1)} \left( \frac{x^p - 1}{x} \right)
\]

irreducible polynomial over \( F_{3^s} \), where \( g^{(1)}(x) \) is the minimal polynomial of \( \alpha^2 \in F_{q^n} \), but with the same analogy we can construct over \( F_{(2^m+1)^s} \) field.

REFERENCES