Two Methods for Constructing Irreducible Polynomials over Finite Fields based on Polynomial Composition

Melsik K. Kyureghyan
Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail: melsik@ipia.sci.am

Mikayel G. Evoyan
Department of Informatics and Applied Mathematics,
Yerevan State University,
Yerevan, Armenia
e-mail: mikhael.ipm@gmail.com

ABSTRACT
The purpose of this paper is to propose constructions of irreducible polynomials over finite fields using composition method. We prove a theorem that extends the class of composition methods of constructing irreducible polynomials over finite fields. Two methods to construct explicitly irreducible polynomials over the Galois field of degrees $q^n - 1$ and $n(q^n + 1)$, where $n$ is a natural number, are developed.

Keywords
Finite field, irreducible polynomial, primitive element, set of coefficients, linear dependence

1. INTRODUCTION
Let $F_q$ be the Galois field of order $q = p^s$, where $p$ is a prime and $s$ is a natural number, $F_q^*$ be its multiplicative group, and let $f(x)$ be a monic irreducible polynomial of degree $n$ over $F_q$ and $\beta$ be a root of $f(x)$. The field $F_q(\beta)$ is a one-dimensional extension of $F_q$ and can be viewed as a vector space of dimension $n$ over $F_q$. The Galois group of $F_q(\beta)$ over $F_q$ is cyclic and is generated by Frobenius mapping $\sigma(\alpha) = \alpha^q$, $\alpha \in F_q$.

We say that the degree of an element $\alpha \in F_q^*$ over $F_q$ is equal to $k$, or equivalently, $\alpha$ is a proper element in $F_q^*$ if $\alpha \in F_q^*$ and $\alpha \not\in F_q^*$, for any proper divisor $\nu$ of $k$, and write $\deg_q(\alpha) = k$.

Similarly, we say that the degree of a subset $A = \{\alpha_1, \alpha_2, \ldots, \alpha_r\} \subset F_q^*$ over $F_q$ is equal to $k$ if for any proper divisor $\nu$ of $k$ there exists at least one element $\alpha_u \in A$ such that $\alpha_u \not\in F_q^*$, and write $\deg_q(A, \{\alpha_1, \alpha_2, \ldots, \alpha_r\}) = k$.

1 We recall that a proper divisor of a natural number $n$ is a divisor of $n$ other than $n$ itself.

2. PRELIMINARIES
For $0 \leq a \leq k - 1$ and any polynomial $g(x) = \sum_{u=0}^{m} b_u x^u$ of degree $m$ in the ring $F_q[x]$ let

$$g^{(a)}(x) = \sum_{u=0}^{m} b_u x^{u+a}.$$  

Further we shall need several auxiliary results.

**Lemma 1** Let $n = dk$ and $f(x)$ be a monic irreducible polynomial of degree $n$ over $F_q$ and let $g(x)$ be a monic irreducible divisor of degree $k$ of $f(x)$ in $F_q[x]$. Then the polynomials $g^{(v)}(x)$ of degree $k$, where $0 \leq v \leq d - 1$, are irreducible over $F_q$ and $f(x)$ has a factorization of the form

$$f(x) = \prod_{v=0}^{d-1} g^{(v)}(x),$$  

where $g^{(0)}(x) = g(x)$ in $F_q[x]$.

**Lemma 2** Let $f(x)$ be a monic irreducible polynomial of degree $kn$ over $F_q$. Then $k$ distinct irreducible polynomials $g^{(v)}(x) = \sum_{u=0}^{n} g_{v,u} x^u$ of degree $n$ over $F_q$ occur in the canonical factorization of
\[ f(x) = \prod_{v=0}^{n-1} g^{(v)}(x) \text{ in } \mathbb{F}_{q^n}[x] \] and the degree of the set of coefficients
\[ \deg_q \left\{ g_0^{q^v}, g_1^{q^v}, \ldots, g_n^{q^v} \right\} \text{ over } \mathbb{F}_q \] of each of these polynomials is equal to \( k \), i.e.
\[ \deg_q \left\{ g_0^{\beta^v}, g_1^{\beta^v}, \ldots, g_n^{\beta^v} \right\} = k. \]

Lemma 3 Let \( g(x) \) be a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \). Then \( g(x) \) is irreducible over \( \mathbb{F}_{q^d} \). Then the degree of the set of coefficients over \( \mathbb{F}_{q^d} \) is equal to \( d \). Then
\[ f(x) = \prod_{v=0}^{n-1} g^{(v)}(x) \text{ of degree } d \] is irreducible over \( \mathbb{F}_{q^d} \).

Lemma 4 Let \( n \) and \( k \) be two natural numbers satisfying the condition \( \gcd(n,k) = 1 \). Then \( f(x) \) is an irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \), and let \( \alpha \) be a nonzero and \( \beta \) an arbitrary element of \( \mathbb{F}_{q^k} \). Then the polynomial \( g(x) = f(\alpha x + \beta) \) is irreducible over \( \mathbb{F}_{q^k} \).

Lemma 5 Let \( n > 1 \) be a prime which does not divide \( q \) and \( r - 1 \) be the order to which \( q \) modulo \( r \) belongs (i.e., \( q^{r-1} \equiv 1 \pmod{r} \)). Let \( f(x) \) be any irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \). Then the degree of the set of coefficients \( \{g_0^\beta, g_1^\beta, \ldots, g_n^\beta\} \) of \( g(x) = f(\alpha x + \beta) \) is irreducible over \( \mathbb{F}_{q^r} \).

Theorem 1 Let \( \Theta \) be a primitive element of \( \mathbb{F}_q \), \( \beta \) be any element of \( \mathbb{F}_q \), and \( p^m > 2 \), where \( m \) divides \( s(q = p^s) \). Then the polynomial
\[ f(x) = x^{p^m} - \Theta x + \beta \]
is the product of a linear polynomial and an irreducible polynomial of degree \( p^m - 1 \) over \( \mathbb{F}_q \).

Theorem 2 ([1], Dickson’s theorem) Let \( q \) be a primitive element of \( \mathbb{F}_q \) and let \( \beta \) be any element of \( \mathbb{F}_q \). Then the polynomial
\[ f(x) = x^{q^n} - x - 1 \]
is the product of a linear polynomial and an irreducible polynomial of degree \( q^n - 1 \) over \( \mathbb{F}_q \).

Theorem 3 Let \( q^n > 2 \) be a primitive polynomial of degree \( n \) over \( \mathbb{F}_q \), and let \( \beta, \gamma \) be some elements of \( \mathbb{F}_q \) such that \( \beta \equiv \gamma \pmod{q^n - 1} \). Then the polynomial
\[ f(x) = (x - \gamma)^s f((x - \gamma)^{-1})(x^{\alpha^s} + \beta) \times (h^s(x - \gamma)^{-1}) \]
is the product of a linear polynomial and an irreducible polynomial of degree \( n(q^n - 1) \) over \( \mathbb{F}_q \).

2 We recall that the order of the polynomial \( f(x) \) is sometimes also called the period of \( f(x) \) or the exponent of \( f(x) \).
PROOF Let $\alpha$ be a root of $f(x) = 0$. Then from the irreducibility of $f(x)$ over $F_q$, it follows that $f(x)$ can be written as

$$f(x) = \prod_{\alpha \in F_q} (x - \alpha^e)$$

over $F_q$.

Substituting $(x - \gamma)^{-1} (x^e + \beta)$ for $x$ in (1), and multiplying both sides of the equation by $(x - \gamma)^e$, we get

$$(x - \gamma)^e f((x - \gamma)^{-1} (x^e + \beta)) = \prod_{\alpha \in F_q} ((x^e + \beta) - \alpha^e x + \beta + \gamma \alpha^e)$$

(2)

Since $q^n > 2$ and $\alpha^e$ is a primitive element in $F_q$, then according to Dickson's theorem, each of the polynomials $x^e - \alpha^e x + \beta + \gamma \alpha^e$ is the product of a linear polynomial and an irreducible polynomial of degree $q^n - 1$ over $F_q$. Note that it is easy to find the root $\theta^e$ of the polynomial $x^e - \alpha^e x + \beta + \gamma \alpha^e$ in $F_q$. Indeed, if $\theta \in F_q$, we have $\theta^e = \theta^e (u = 0, 1, \ldots, n - 1)$, and so $\theta^e (\alpha^e - 1) = \beta + \gamma \alpha^e$ if and only if $\theta^e = (\beta + \gamma \alpha^e) (\alpha^e - 1)^{-1}$. Then $x^e - \alpha^e x + \beta + \gamma \alpha^e = x^e - \alpha^e x + \theta^e (\alpha^e - 1) = (x - \theta^e) (x^{e-1} + \theta^e x^{e-2} + \theta^e x^{e-3} + \cdots + \theta^e (\alpha^e - 1)) = (x - \theta^e) Q^e(x)$.

Where $u = 0, 1, \ldots, n - 1$. The expression

$$x^e - \alpha^e x + \beta + \gamma \alpha^e = x^e - \alpha^e x + \theta^e (\alpha^e - 1) = (x - \theta^e) Q^e(x)$$

follows directly from (2).

It can be clearly seen that each of the polynomials $Q^e(x)$ has at least one coefficient, say $\theta^e$ or $1 - \alpha^e$, which is a proper element of $F_q$, and therefore the polynomial $F(x) = \prod_{u=0}^{n-1} Q^e(x)$ is irreducible over $F_q$ by Lemma 3.

Thus, because $\theta$ is a proper element of $F_q$, we obtain

$$(x - \gamma)^e f((x - \gamma)^{-1} (x^e + \beta)) = H(x) F(x),$$

where $H(x) = \prod_{u=0}^{n-1} (x - \theta^e)$. We now show that

$$\prod_{u=0}^{n-1} (x - \theta^e) = H(x) = h^e (x - \gamma).$$

Indeed, since $\theta^e (\alpha^e - 1) = \beta + \gamma \alpha^e$ or, equivalently, $\theta^e (\alpha^e - 1) = \beta + \gamma + \gamma \alpha^e - 1$ we have that $\theta^e = (\beta + \gamma) (\alpha^e - 1)^{-1} + \gamma$. And because $\beta + \gamma + (\alpha^e - 1)$ is a root of $h(x) = f((\beta + \gamma) x + 1)$, then $(\beta + \gamma (\alpha^e - 1))$ is a root of $h^e (x)$. Thus $\theta^e$ is a root of $h^e (x - \gamma)$. □

Later on we shall describe another method that allows explicit constructions of irreducible polynomials of degrees $n(q^n + 1)$ over Galois fields based on Sidelnikov’s results.

Theorem 4 (Sidelnikov [3]) The polynomial $f(x) = x^{q^n + 1} - \alpha x^{q^n} - (x_1 + x_0 - \omega) x + 1$ where $x_1 = x_0^q$, $x_0 \in F_q$, $x_0^{q+1} = 1$, $\omega \in F_q$ is an irreducible polynomial if and only if $\theta = x_1 - x_0$ is a generating element of the group $\Pi$, where $\Pi$ is the set of roots of the equation $y^{q+1} = 1$, and the polynomial $f(x)$ has linearly independent roots.

We apply the theorem above to derive the following result.

Theorem 5 Let $f(x)$ be an irreducible polynomial of degree $2n$ over $F_q$ belonging to the exponent $e(q^n + 1)$, $x^{q^n} - x^e + 1 \equiv R(x) (\mod f(x))$ and $\psi(x) = \sum_{u=0}^n \psi_u x^u$, where $\psi(x)$ is the nonzero polynomial of the least degree satisfying the congruence

$$\sum_{u=0}^n \psi_u (R(x))^u \equiv 0 (\mod f(x)).$$

Then the polynomials $\psi(x)$ and

$$F(x) = x^e \psi(x^{q^n + 1} + x^e + 1)$$

of degrees $n$ and $n(q^n + 1)$, respectively, are irreducible over $F_q$.

PROOF Let $\alpha$ be a root of the equation $f(x) = 0$. Since $f(x)$ is an irreducible polynomial of degree $2n$ over $F_q$ belonging to the exponent $e(q^n + 1)$ by hypothesis, we have that $\alpha^{e(q^n + 1)} = \beta^{q^n + 1} = 1$, where $\beta = \alpha^e$. We know that if $\theta$ is an element of the
extension field of $F_q$ and the degree of the minimal polynomial of $\theta$ is equal to $k$, then the order of $\theta$ divides $q^k - 1$, but does not divide a smaller number $q^j - 1$. In our case since the order $q^n + 1$ of $\beta$ divides $q^{2n} - 1$, but does not divide a smaller number $q^j - 1$, then the degree of the minimal function of $\beta$ over $F_q$ is $2n$, i.e. $\text{deg}_q(\beta) = 2n$. Because $\beta \in F_{q^{2n}}$, it is clearly seen that $\beta^{q^n} + \beta + 1 = 0$, and so $\beta^{q^n} + \beta + 1 \in F_q$. Show now that $\beta^{q^n} + \beta + 1$ is a proper divisor of $\beta^{q^n + \gamma} + \beta^{q^n} + \gamma \beta + \beta^2 = \beta^{q^n + 1}$. Then $\beta^{q^n + \gamma} + \beta^{q^n} + \gamma \beta + \beta^2 = \beta^{q^n + 1} = 1$. 

Next let $G(x)$ be the minimal polynomial of $\beta$ over $F_q$. By Lemma 1 the polynomial $G(x) = \prod_{v=0}^{d-1} g^{(v)}(x)$, where $g^{(v)}(x)$ are polynomials of degree $\frac{2n}{d}$ over $F_{q^d}$. Since $\beta$ is a root of $G(x)$, then $\beta$ is also a root of one of the polynomials $g^{(v)}(x)$, say, without loss of generality, a root of $g^{(0)}(x) = g(x)$. Then $g(x)$ is the minimal polynomial of $\beta$ over $F_{q^d}$. And since $\beta$ is also a root of the polynomial $x^2 + (1 - \gamma)x + 1$ over $F_{q^d}$, which implies that $g(x)$ divides $x^2 + (1 - \gamma)x + 1$, we arrive at a contradiction as the degree of the minimal polynomial $g(x)$ of $\beta$ over $F_{q^d}$ is equal to $\frac{2n}{d} > 2$.

Thus $\beta^{q^n} + \beta + 1$ is a proper element in $F_{q^d}$, which establishes the irreducibility of the polynomial $\psi(x) = \prod_{v=0}^{n-1} \left(x - \left(\beta^{q^n} + \beta + 1\right)^v\right)$ over $F_q$. Since $f(x)$ is an irreducible polynomial of degree $2n$ over $F_q$ by hypothesis, then it is easily seen that the congruence $x^{q^n} + x^n + 1 \equiv R(x) \mod f(x)$ is equivalent to the relation $\alpha^{q^n} + \alpha^n + 1 = R(\alpha)$ in $F_{q^{2n}}$ or $\beta^{q^n} + \beta + 1 = R(\alpha)$, where $\beta = \alpha^n$. Hence $\psi(x)$ is again the minimal polynomial of $R(\alpha)$ over $F_q$, or equivalently $\psi(x)$ is the nonzero polynomial of the least degree satisfying congruence (3). Next we show that the conditions of Theorem 4 are satisfied under hypothesis of Theorem 5. Indeed, since $\beta \in F_{q^{2n}} | F_q$, then for $x_0 = \beta$ and $x_1 = \beta^{q^n}$ we have $x_1 = x_0^{q^n}$, $x_0 \in F_{q^{2n}} | F_q$, $x_0^{q^n + 1} = 1$, and for $\omega = -1$ the element $\omega - x_1 = -1 - \beta^{q^n} = \beta^{q^n}$ is a generating element of $\Pi$, where $\Pi$ is the set of roots of the equation $\gamma^{q^n + 1} = 1$. Thus the conditions of Sidelnikov theorem are satisfied. Hence by Theorem 7 the polynomial $x^{q^n + 1} + x^n - (\beta^{q^n} + \beta + 1)x + 1$ is irreducible over $F_{q^n}$, since the coefficients of the polynomial belong to $F_{q^d}$.

Next substituting $\frac{x^{q^n + 1} + x^n + 1}{x}$ for $x$ in (3), and multiplying both sides of the expression by $x$, we obtain

$$\psi\left(x^{q^n + 1} + x^n + 1\right)$$

$$= \prod_{u=0}^{n-1} \left(x^{q^n + 1} + x^n - (\beta^{q^n} + \beta + 1)x + 1\right).$$

However, by Lemma 3, the polynomial $x^n \psi\left(x^{q^n + 1} + x^n + 1\right)$ is irreducible over $F_q$, since the polynomial $x^{q^n + 1} + x^n - (\beta^{q^n} + \beta + 1)x + 1$ is irreducible over $F_{q^n}$, and $\text{deg}_q(\beta^{q^n} + \beta + 1) = n$. □

REFERENCES