

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

We say that the degree of an element $\alpha \in \mathbf{F}_{q^k}$ over \mathbf{F}_q is equal to k , or equivalently, α is a proper element in \mathbf{F}_{q^k} if $\alpha \in \mathbf{F}_{q^k}$ and $\alpha \notin \mathbf{F}_{q^v}$ for any proper divisor v of k , and write $\mathbf{deg}_q(\alpha) = k$.

Similarly, we say that the degree of a subset $A = \{\alpha_1, \alpha_2, \dots, \alpha_r\} \subset \mathbf{F}_{q^k}$ over \mathbf{F}_q is equal to k if for any proper divisor v of k there exists at least one element $\alpha_u \in A$ such that $\alpha_u \notin \mathbf{F}_{q^v}$, and write $\mathbf{deg}_q\{\alpha_1, \alpha_2, \dots, \alpha_r\} = k^1$.

Constructing explicitly irreducible polynomials of high degrees is a challenging problem in the constructive theory of finite fields. In this paper we obtain two methods to construct explicitly irreducible polynomials over the Galois field \mathbf{F}_q of degrees $n(q^n - 1)$ and $n(q^n + 1)$, where n is a natural number. These constructions are based upon operator substitutions in $\mathbf{F}_q[x]$ derived by Varshamov in [4], Dickson [1,2] and Sidelnikov [3]. Throughout this paper we will consider only monic polynomials, i.e. polynomials whose leading coefficient is equal to 1.

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 $\mathbf{F}_{q^k}[x]$ let

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

Further we shall need several auxiliary results.

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

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

in $\mathbf{F}_{q^d}[x]$.

Lemma 2 Let $f(x)$ be a monic irreducible polynomial of degree kn over \mathbf{F}_q . Then k distinct irreducible

polynomials $g^{(v)}(x) = \sum_{u=0}^n g_u^{q^v} x^u$ of degree n over

\mathbf{F}_{q^k} occur in the canonical factorization of

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

$f(x) = \prod_{v=0}^{k-1} g^{(v)}(x)$ in $\mathbf{F}_{q^d}[x]$ and the degree of the set of coefficients

$\deg_q \{g_0^{q^v}, g_1^{q^v}, \dots, g_n^{q^v}\}$ over \mathbf{F}_q of each of these polynomials is equal to k , i.e. $\deg_q \{g_0^{q^v}, g_1^{q^v}, \dots, g_n^{q^v}\} = k$.

Lemma 3 Let $g(x)$ be a monic irreducible polynomial of degree n over \mathbf{F}_{q^d} the degree of the set of whose coefficients over \mathbf{F}_q is equal to d . Then

$f(x) = \prod_{v=0}^{d-1} g^{(v)}(x)$ of degree dn is irreducible over \mathbf{F}_q with $g^{(0)}(x) = g(x)$.

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

Lemma 5 Let $n > 1$, $F = 1, 2, 3$ and k be natural numbers satisfying the condition $\mathbf{gcd}(n, k) = 1$, $f(x)$ be an irreducible polynomial of degree n over \mathbf{F}_q , and let α be a nonzero and β an arbitrary element of \mathbf{F}_{q^k} satisfying the conditions: $\deg_q(\alpha) = k^{\varepsilon_1}$,

$\deg_q(\beta) = k^{\varepsilon_2}$, $\deg_q(\alpha^{-1}\beta) = k^{\varepsilon_3}$ and $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 > 0$, where $\varepsilon_i = 0$ or 1 ($i = 1, 2, 3$). Then the degree of the set of coefficients $\{g_0, g_1, \dots, g_n\}$ of the polynomial $g(x) = f(\alpha x + \beta)$ is equal to k over \mathbf{F}_q , i.e.

$\deg_q \{g_0, g_1, \dots, g_n\} = k$.

We apply Lemmas 1, 2 and 3 to derive the following result.

Theorem 1 Let $p^S = q$, $n > 1$ and k be natural numbers, $\mathbf{gcd}(n, k) = 1$, $f(x)$ be an irreducible polynomial of degree n over \mathbf{F}_q , and let α be a nonzero and β an element of \mathbf{F}_{q^k} under the conditions

of Lemma 5, $f(\alpha x + \beta) = g(x) = \sum_{u=0}^n g_u x^u$. Then

the polynomial $g^{(a)}(x) = \sum_{u=0}^n g_u^{q^a} x^u$ of degree nk

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

where $g^{(a)}(x) = \sum_{u=0}^n g_u^{q^a} x^u$ is irreducible over \mathbf{F}_q .

Corollary 1 Let r be a prime which does not divide q and $r-1$ be the order to which q modulo r belongs (i.e. $q^{r-1} \equiv 1 \pmod{r}$, $0 < j < r-1$, $q^j \not\equiv 1 \pmod{r}$); also let $f(x)$ be any irreducible polynomial of degree $n > 1$ over \mathbf{F}_q belonging to

order² t , $x^r \equiv R(x) \pmod{f(x)}$ and

$\psi(x) = \sum_{u=0}^n \psi_u x^u$, where $\psi(x)$ is the nonzero polynomial of minimal degree satisfying the congruence

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

and $\mathbf{gcd}(n, r-1) = 1$. Then the polynomial

$$F(x) = f^{-1}(x) \psi(x^r)$$

of degree $(r-1)n$ is irreducible over \mathbf{F}_q and belongs to order rt .

3. IREDICIBILITY OF POLYNOMIAL COMPOSITIONS

Further we provide a method that enables explicit constructions of irreducible polynomials of degree $n(q^n - 1)$ from given primitive polynomials of degree n by using a simple transformation. The method is based upon the following result.

Theorem 2 ([1], Dickson's theorem) Let θ be a primitive element of \mathbf{F}_q , β be any element of \mathbf{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 \mathbf{F}_q .

Theorem 3 Let $q^n > 2$, $f(x) \neq x - 1$ be a primitive polynomial of degree n over \mathbf{F}_q , and let β, γ be some elements of \mathbf{F}_q such that $\beta \equiv \mp \gamma$, $h(x) = f((\beta + \gamma)x + 1)$, $h^*(x) = x^n h(\frac{1}{x})$. Then the polynomial

$$F(x) = (x - \gamma)^n f((x - \gamma)^{-1} (x^{q^n} + \beta)) \times (h^*(x - \gamma))^{-1}$$

of degree $n(q^n - 1)$ is irreducible over \mathbf{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 α be a root of $f(x) = 0$. Then from the irreducibility of $f(x)$ over \mathbf{F}_q it follows that $f(x)$ can be written as

$$f(x) = \prod_{u=0}^{n-1} (x - \alpha^{q^u}) \quad (1)$$

over \mathbf{F}_{q^n} .

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

$$\begin{aligned} & (x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right) \\ &= \prod_{u=0}^{n-1} (x^{q^n} - \alpha^{q^u} x + \beta + \gamma \alpha^{q^u}). \end{aligned} \quad (2)$$

Since $q^n > 2$ and α^{q^u} is a primitive element in \mathbf{F}_{q^n} , then according to Dickson's theorem, each of the polynomials $x^{q^n} - \alpha^{q^u} x + \beta + \gamma \alpha^{q^u}$ is the product of a linear polynomial and an irreducible polynomial of degree $q^n - 1$ over \mathbf{F}_{q^n} . Note that it is easy to find the

root θ^{q^u} of the polynomial $x^{q^n} - \alpha^{q^u} x + \beta + \gamma \alpha^{q^u}$ in \mathbf{F}_{q^n} . Indeed, if $\theta \in \mathbf{F}_{q^n}$,

we have $\theta^{q^{n+u}} = \theta^{q^u}$ ($u = 0, 1, \dots, n-1$), and so $\theta^{q^u}(\alpha^{q^u} - 1) = \beta + \gamma \alpha^{q^u}$ if and only if $\theta^{q^u} = (\beta + \gamma \alpha^{q^u})(\alpha^{q^u} - 1)^{-1}$. Then

$$\begin{aligned} x^{q^n} - \alpha^{q^u} x + \beta + \gamma \alpha^{q^u} &= x^{q^n} - \alpha^{q^u} x \\ &+ \theta^{q^u}(\alpha^{q^u} - 1) = x^{q^n} - \theta^{q^{n+u}} - \alpha^{q^u} (x - \theta^{q^u}) \\ &= (x - \theta^{q^u}) (x^{q^n-1} + \theta^{q^u} x^{q^n-2} + \theta^{2q^u} x^{q^n-3} + \dots \\ &+ \theta^{(q^n-2)q^u} x + 1 - \alpha^{q^u}) = (x - \theta^{q^u}) Q^{(u)}(x), \end{aligned}$$

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

$$\begin{aligned} & (x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right) \\ &= \prod_{u=0}^{n-1} (x - \theta^{q^u}) Q^{(u)}(x) \end{aligned}$$

follows directly from (2).

It can be clearly seen that each of the polynomials $Q^{(u)}(x)$ has at least one coefficient, say θ^{q^u} or $1 - \alpha^{q^u}$ which is a proper element of \mathbf{F}_{q^n} , and

therefore the polynomial $F(x) = \prod_{u=0}^{n-1} Q^{(u)}(x)$ is irreducible over \mathbf{F}_q by Lemma 3.

Thus, because θ is a proper element of \mathbf{F}_{q^n} , we obtain

$$(x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right) = H(x)F(x),$$

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

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

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

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 Sidelnokov's results.

Theorem 4 (Sidelnokov [3]) The polynomial

$$f(x) = x^{q^2+1} - \omega x^q - (x_0 + x_1 - \omega)x + 1$$

where $x_1 = x_0^q$, $x_0 \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, $x_0^{q^2+1} = 1$, $\omega \in \mathbf{F}_q$ is

an irreducible polynomial if and only if $\frac{\omega - x_1}{\omega - x_0}$ is a

generating element of the group Π , where Π is the set of roots of the equation $y^{q^2+1} = 1$, 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 \mathbf{F}_q belonging to the exponent

$$e(q^n + 1), \quad x^{e q^n} + x^e + 1 \equiv R(x) \pmod{f(x)}$$

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

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

Then the polynomials $\psi(x)$ and

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

of degrees n and $n(q^n + 1)$, respectively, are irreducible over \mathbf{F}_q .

PROOF Let α be a root of the equation $f(x) = 0$. Since $f(x)$ is an irreducible polynomial of degree $2n$ over \mathbf{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 θ is an element of the

extension field of \mathbf{F}_q and the degree of the minimal polynomial of θ is equal to k , then the order of θ divides $q^k - 1$, but does not divide a smaller number $q^i - 1$. In our case since the order $q^n + 1$ of β divides $q^{2n} - 1$, but does not divide a smaller number $q^i - 1$, then the degree of the minimal function of β over \mathbf{F}_q is $2n$, i.e. $\deg_q(\beta) = 2n$. Because $\beta \in \mathbf{F}_{q^{2n}}$, it is clearly seen

that $(\beta^{q^n} + \beta + 1)^{q^n} = \beta^{q^n} + \beta + 1$, and so $\beta^{q^n} + \beta + 1 \in \mathbf{F}_{q^n}$. Show now that $\beta^{q^n} + \beta + 1$ is a proper element of \mathbf{F}_{q^n} . Suppose, on the contrary, that

the maximal degree of $\beta^{q^n} + \beta + 1$ over \mathbf{F}_{q^n} is equal to d , i.e. $\deg_q(\beta^{q^n} + \beta + 1) = d$, where d is a proper divisor of n . Then if $\beta^{q^n} + \beta + 1 = \gamma \in \mathbf{F}_{q^d}$

we have $\beta^{q^{n+1}} + \beta^2 + \beta = \gamma\beta$ or $\beta^2 + (1 - \gamma)\beta + 1 = 0$ in $\mathbf{F}_{q^{2n}}$ since $\beta^{q^{n+1}} = 1$.

Now let $G(x)$ be the minimal polynomial of β over \mathbf{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 \mathbf{F}_{q^d} . Since β is a root of $G(x)$,

then β 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 β over \mathbf{F}_{q^d} . And since β is also a root

of the polynomial $x^2 + (1 - \gamma)x + 1$ over \mathbf{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 β over \mathbf{F}_{q^d} is equal to $\frac{2n}{d} > 2$.

Thus $\beta^{q^n} + \beta + 1$ is a proper element in \mathbf{F}_{q^n} , which establishes the irreducibility of the polynomial

$$\psi(x) = \prod_{u=0}^{n-1} \left(x - (\beta^{q^n} + \beta + 1)^{q^u} \right) \quad (3)$$

over \mathbf{F}_q . Since $f(x)$ is an irreducible polynomial of degree $2n$ over \mathbf{F}_q by hypothesis, then it is easily seen that the congruence $x^{eq^n} + x^e + 1 \equiv R(x) \pmod{f(x)}$ is equivalent to

the relation $\alpha^{eq^n} + \alpha^e + 1 = R(\alpha)$ in $\mathbf{F}_{q^{2n}}$ or

$\beta^{q^n} + \beta + 1 = R(\alpha)$, where $\beta = \alpha^e$. Hence

$\psi(x)$ is again the minimal polynomial of $R(\alpha)$ over \mathbf{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 $\beta \in \mathbf{F}_{q^{2n}} \setminus \mathbf{F}_{q^n}$ then for $x_0 = \beta$ and $x_1 = \beta^{q^n}$ we

have $x_1 = x_0^{q^n}$, $x_0 \in \mathbf{F}_{q^{2n}} \setminus \mathbf{F}_{q^n}$, $x_0^{q^{n+1}} = 1$, and for

$\omega = -1$ the element $\frac{\omega - x_1}{\omega - x_0} = \frac{-1 - \beta^{q^n}}{-1 - \beta} = \beta^{q^n}$ is a

generating element of Π , where Π is the set of roots of

the equation $y^{q^n+1} = 1$. Thus the conditions of Sidelnikov theorem are satisfied. Hence by Theorem 7

the polynomial $x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1$ is irreducible over \mathbf{F}_{q^n} since the coefficients of the polynomial belong to \mathbf{F}_{q^n} .

Next substituting $\frac{x^{q^n+1} + x^{q^n} + 1}{x}$ for x in (3), and

multiplying both sides of the expression by x^n , we obtain

$$\begin{aligned} & x^n \psi \left(\frac{x^{q^n+1} + x^{q^n} + 1}{x} \right) \\ &= \prod_{u=0}^{n-1} \left(x^{q^{n+1}+1} + x^{q^n} - (\beta^{q^{n+u}} + \beta^{q^n} + 1)x + 1 \right). \end{aligned}$$

However, by Lemma 3, the polynomial

$x^n \psi \left(\frac{x^{q^n+1} + x^{q^n} + 1}{x} \right)$ is irreducible over \mathbf{F}_q , since

the polynomial $x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1$ is irreducible over \mathbf{F}_{q^n} and $\deg_q(\beta^{q^n} + \beta + 1) = n$. \square

REFERENCES

- [1] A. A. Albert. *Fundamental Concepts of Higher Algebra*. University of Chicago Press, 1956.
- [2] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1987.
- [3] V. M. Sidelnikov, "On normal bases of a finite field", *Math. USSR Sbornik*, pp. 485–494, 61(1988).
- [4] R. R. Varshamov, "A general method of synthesizing irreducible polynomials over Galois fields", *Soviet Math. Dokl.*, pp. 334–336, 29(1984).
- [5] N. Zierler, "Linear recurring sequences", *J. Soc. Ind. Appl. Math.* 7, N1, pp. 31–48, (1959).