Finite Fields and Their Applications **8,** 52–68 (2002)
doi.10.1006/ffta.2001.0323, available online at http://www.idealibrary.com on IDEAL®

Recurrent Methods for Constructing Irreducible Polynomials over $GF(2^s)$

Mels K. Kyuregyan

Institute for Informatics and Automation Problems, Armenian National Academy of Sciences, P. Sevak str. 1, 375044 Yerevan, Armenia
E-mail: kyuregm@forof.sci.am

Communicated by Stephen D. Cohen

Received May 17, 1999; revised December 6, 2000; published online July 11, 2001

The paper is devoted to some results concerning the constructive theory of the synthesis of irreducible polynomials over Galois fields $GF(q)$, $q = 2^s$. New methods for the construction of irreducible polynomials of higher degree over $GF(q)$ from a given one are worked out. The complexity of calculations does not exceed $O(n^3)$ single operations, where n denotes the degree of the given irreducible polynomial. Furthermore, a recurrent method for constructing irreducible (including self-reciprocal) polynomials over finite fields of even characteristic is proposed.
Key Words: irreducible polynomials; operator; Galois fields; recurrent method; primitive element; root; great common divisor; mapping; exponent.

This paper presents some results on the constructive theory of the synthesis of irreducible polynomials over $GF(2^s)$. The problem of reducibility of polynomials over Galois fields is a case of special interest [1, 11, 12] and plays an important role in modern engineering [4, 10, 13]. In particular, since the binary system of notation is mainly used in computing systems, the problem of the construction of irreducible polynomials over $GF(2^s)$ remains one of the most important ones from practical point of view.

Let $GF(q)$ be the Galois field of order $q = p^s$, where p is a prime and s is a natural number.

The *degree of an element* α *over the field* $GF(q)$ is said to be equal to k or α is said to be a *proper element* of the field $GF(q^k)$ if $\alpha \in GF(q^k)$ and $\alpha \notin GF(q^v)$ for any proper divisor v of k. In this case we write $\deg_q(\alpha) = k$.

Similarly, the *degree of a subset* $A = \{\alpha_1, \alpha_2, \ldots, \alpha_r) \subset GF(q^k)$ over the field $GF(q)$ is said to be equal to k if for any proper divisor v of k there exists at least an element $\alpha_u \in A$ such that $\alpha_u \notin GF(q^v)$. In this case we write $\deg_q [\alpha_1, \alpha_2, \ldots, \alpha_r\} = k$.

Only monic polynomials, i.e., the polynomials whose leading coefficient is equal to 1, are studied in this paper.

We will use the results obtained by Shwarz in [5] and [2] to prove the following fact.

THEOREM 1. *Let $f(x) = \sum_{u=0}^{n} c_u x^u$ be an irreducible polynomial over $GF(q)$, δ, $\delta_1 \in GF(q)$, $\delta \neq 0$ and*

$$x^{(p^{sn}-1)/(p-1)} \equiv 1 \pmod{f(x-\delta_1)}. \tag{1}$$

Then the polynomial

$$g(x) = x^n f\left(\frac{x^p - \delta_1 x - \delta}{x}\right)$$

of degree n is irreducible over $GF(q)$ if and only if the following relation holds

$$\sum_{u=0}^{sn-1} \delta^{p^u} x^{(p^{ns} - p^{u+1})/(p-1)} \not\equiv 0 \pmod{f(x-\delta_1)}. \tag{2}$$

Otherwise $g(x)$ factors as the product of a p irreducible polynomials of degree n.

Proof. By using the irreducibility of $f(x)$ over $GF(q)$, we have the following relation over $GF(q^n)$

$$f(x) = \prod_{u=0}^{n-1} (x - \alpha^{q^u}). \tag{3}$$

Substituting $(x^p - \delta_1 x - \delta)/x$ for x in (3) and multiplying both sides by x^n, we obtain

$$g(x) = \prod_{u=0}^{n-1} (x^p - (\delta_1 + \alpha)^{q^u} x - \delta). \tag{4}$$

By [5], the polynomial $x^p - (\delta_1 + \alpha)x - \delta$ is irreducible over $GF(q^n)$ if both the conditions $(\delta_1 + \alpha)^{(p^{sn}-1)/(p-1)} = 1$ and

$$\frac{\delta}{\delta_1 + \alpha} + \frac{\delta^p}{(\delta_1 + \alpha)^{1+p}} + \frac{\delta^{p^2}}{(\delta_1 + \alpha)^{1+p+p^2}} + \cdots + \frac{\delta^{p^{sn-1}}}{(\delta_1 + \alpha)^{1+p+p^2+\cdots+p^{sn-1}}}$$
$$= \sum_{u=0}^{sn-1} \delta^{p^u} (\delta_1 + \alpha)^{(p^{ns} - p^{u+1})/(p-1)} \neq 0$$

are satisfied. Then it follows from [2] that $g(x)$ is irreducible over $GF(q)$. Hence if both conditions (1) and (2) are satisfied then $g(x)$ is irreducible over $GF(q)$.

By [5] the polynomial $x^p - (\delta_1 + \alpha)x - \delta$ (where $(\delta_1 + \alpha)^{(p^{sn}-1)/(p-1)} = 1$) factors into a product of p linear factors (i.e., we have a relation of the form

$$x^p - (\delta_1 + \alpha)x - \delta = \prod_{v=1}^{p} (x - \beta_v))$$

if and only if

$$\sum_{u=0}^{sn-1} \delta^{p^u}(\delta_1 + \alpha)^{(p^{ns} - p^{u+1})/(p-1)} = 0.$$

Then it is evident that

$$x^p - (\delta_1 + \alpha)^{q^u} x - \delta = \prod_{v=1}^{p} (x - \beta_v^{q^u}). \tag{5}$$

From relations (4) and (5) we have that

$$g(x) = \prod_{v=1}^{p} \prod_{u=0}^{n-1} (x - \beta_v^{q^u}),$$

whereas it follows that $g(x)$ factors as the product of p co-factors if and only if both (1) and the condition

$$\sum_{u=0}^{sn-1} \delta^{p^u} x^{(p^{ns} - p^{u+1})/(p-1)} \equiv 0 \pmod{f(x - \delta_1)}$$

are satisfied. This completes our proof. ■

LEMMA 1. *Let* $f(x) = \sum_{u=0}^{n} c_u x^u$ *be an irreducible polynomial over* $GF(q)$ *that belongs to the exponent e and has at least one nonzero coefficient* c_1, c_{n-1}. *For a divisor t of* $q - 1$, *suppose that*

$$x^t \equiv R(x) \pmod{f(x)}.$$

Also, let $\psi(x) = \sum_{u=0}^{n} \psi_u x^u$, *where* ψ_u *is a nontrivial solution of the relation*

$$\sum_{u=0}^{n} \psi_u (R(x))^u \equiv 0 \pmod{f(x)}. \tag{6}$$

Then the polynomial $\psi(x)$ (of degree n) is irreducible over $GF(q)$ and belongs to the exponent $e/(t, e)$.

Proof. Let α be a root of the equation $f(x) = 0$. By (6), we can easily verify that α^t is the root of $\psi(x)$. It will be sufficient then to show that α^t is the proper element of $GF(q^n)$. So, assume the contrary, namely that $\deg_q(\alpha^t) = d$, where d is a proper divisor of n. Consider separately two cases.

1. Let $c_1 \neq 0$. Since

$$\sum_{u=0}^{n-1} \left(\frac{1}{\alpha}\right)^{q^u} = -\frac{c_1}{c_0} \qquad \text{or} \qquad \frac{1}{\alpha}\sum_{u=0}^{n-1} \left(\frac{1}{\alpha}\right)^{q^u - 1} = -\frac{c_1}{c_0}$$

then, as $t\,|\,(q^u - 1)$, we have $(1/\alpha)^{q^u - 1} \in GF(q^d)$, which implies that $\sum_{u=0}^{n-1} (1/\alpha)^{q^u - 1} \in GF(q^d)$. Also, in view of the fact that

$$\alpha = -\frac{c_0}{c_1} \sum_{u=0}^{n-1} \left(\frac{1}{\alpha}\right)^{q^u - 1} \in GF(q^d),$$

we have $\deg_q(\alpha) < n$, which is impossible.

2. Let $c_{n-1} \neq 0$. Then, since $\sum_{u=0}^{n-1} \alpha^{q^u} = -c_{n-1}$ or $\alpha \sum_{u=0}^{n-1} \alpha^{q^u - 1} = -c_{n-1}$ and as $t\,|\,(q^u - 1)$, we have

$$\alpha = -\left(\sum_{u=0}^{n-1} \alpha^{q^u - 1}\right)^{-1} c_{n-1} \in GF(q^d)$$

and therefore $\deg_q(\alpha) < n$, which is also impossible.

The lemma is proved. ∎

THEOREM 2. *Let $\delta \neq 0$ be an arbitrary element in $GF(q)$ and let $f(x) = \sum_{u=0}^{n} c_u x^u$ be any irreducible polynomial over $GF(q)$ with coefficients satisfying the conditions*

$$\sum_{u=0}^{s-1} \left(\frac{c_1 \delta}{c_0}\right)^{p^u} \neq 0, \quad x^{p-1} \equiv R(x) \pmod{f(x)}, \qquad \textit{and} \qquad \psi(x) = \sum_{u=0}^{n} \psi_u x^u,$$

where ψ_u is a nontrivial solution of the equation

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

Then the polynomial $F(x) = x^n \psi((x^p - \delta^p)/x)$ is irreducible over $GF(q)$.

Proof. By Lemma 1, $\psi(x)$ is irreducible over $GF(q)$ and it is then obvious that $\alpha^{p-1} = \theta$ will be a root of $\psi(x)$. Furthermore, by Theorem 1, $F(x)$ is irreducible over $GF(q)$ if θ and δ satisfy the conditions

$$\sum_{u=0}^{sn-1} \delta^{p^{u+1}} \theta^{(p^{ns}-p^{u+1})/(p-1)} \neq 0 \qquad \text{and} \qquad \theta^{(p^{ns}-1)/(p-1)} = 1.$$

Later we will use the fact that $\theta = \alpha^{p-1}$ to simplify the above given conditions as follows,

$$\sum_{u=0}^{sn-1} \delta^{p^{u+1}} \alpha^{p^{ns}-p^{u+1}} = \alpha\left(\sum_{u=0}^{s-1}\left(\sum_{v=0}^{n-1}\left(\frac{1}{\delta^{-1}\alpha}\right)^{p^{sv}}\right)^{p^u}\right)^p$$

and

$$f(\delta x) = \sum_{u=0}^{n} c_u (\delta x)^u = \sum_{u=0}^{n} h_u x^u,$$

whereas $h_1 = c_1\delta$ and by Vieta's theorem

$$\sum_{u=0}^{s-1}\left(\sum_{v=0}^{n-1}\left(\frac{1}{\delta^{-1}\alpha}\right)^{p^{sv}}\right)^{p^u} = \sum_{u=0}^{s-1}\left(-\frac{c_1\delta}{c_0}\right)^{p^u} \neq 0.$$

Besides, $\theta^{(p^{ns}-1)/(p-1)} = \alpha^{p^{ns}-1} = 1$. Thus if $\sum_{u=0}^{s-1}(-c_1\delta/c_0)^{p^u} \neq 0$, then $F(x)$ is irreducible over $GF(q)$. The theorem is proved. ■

Based on the results obtained above we now give a recurrent method for constructing irreducible polynomials over $GF(2^s)$.

Let $f(x) = \sum_{u=0}^{n} c_u x^u$ be an polynomial of degree n over $GF(2^s)$. Consider the quadratic mapping

$$f(x) \to x^n f\left(\frac{x^2+\delta^2}{x}\right) = \tilde{f}(x) \qquad (\delta \in GF(2^s),\ \delta \neq 0)$$

onto the ring $GF(2^s)\,[x]$. Assume that A is an operator defined over the ring $GF(2^s)\,[x]$ that maps $f(x)$ onto $Af(x) = f((x^2+\delta^2)/x)$, where $\delta \in GF(2^s)$ and $\delta \neq 0$, if $f(x) \in GF(2^s)\,[x]$. Here $A^m f(x)$ $(m > 1)$ signifies $A^m f(x) = A(A^{m-1}f(x))$.

We start our study with the simplest case, when $f(x) = x$. Then we have

$$Ax = \frac{x^2+\delta^2}{x} = \frac{a_1(x)}{b_1(x)},$$

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

$$A^2 x = A\,\frac{a_1(x)}{b_1(x)} = \frac{x^2 A a_1(x)}{x^2 A b_1(x)} = \frac{a_2(x)}{b_2(x)},$$

where

$$a_2(x) = x^2 A(a_1(x)) = a_1^2(x) + (\delta b_1(x))^2,$$

$$b_2(x) = x^2 A b_1(x) = a_1(x) b_1(x).$$

Now, for each integer $m > 1$, set $A^m x = (a_m(x)/b_m(x))$, where

$$\begin{aligned} a_m(x) &= x^{2^{m-1}} A a_{m-1}(x) = a_{m-1}^2(x) + (\delta b_{m-1}(x))^2, \\ b_m(x) &= x^{2^{m-1}} A b_{m-1}(x) = a_{m-1}(x) b_{m-1}(x) \end{aligned} \tag{7}$$

under the initial conditions $a_1(x) = x^2 + \delta^2$ and $b_1(x) = x$.

In this, for $m + 1$, by (7), we have that

$$\begin{aligned} A^{m+1} x = A(A^m x) = A\,\frac{a_m(x)}{b_m(x)} &= A\,\frac{a_{m-1}^2(x) + (\delta b_{m-1}(x))^2}{a_{m-1}(x) b_{m-1}(x)} \\ &= \frac{(x^{2^{m-1}} A a_{m-1}(x))^2 + (\delta x^{2^{m-1}} A b_{m-1}(x))^2}{(x^{2^{m-1}} A a_{m-1}(x))(x^{2^{m-1}} A b_{m-1}(x))} = \frac{a_m^2(x) + (\delta b_m(x))^2}{a_m(x) b_m(x)} \end{aligned}$$

i.e., $A^{m+1} x = a_{m+1}(x)/b_{m+1}(x)$, where

$$a_{m+1}(x) = a_m^2(x) + (\delta b_{m+1}(x))^2,$$

$$b_{m+1}(x) = a_m(x) b_m(x).$$

Thus, by induction, for any m, we have

$$A^m x = \frac{a_m(x)}{b_m(x)},$$

or, in more general form,

$$A^m f(x) = f\left(\frac{a_m(x)}{b_m(x)}\right),$$

where $a_m(x)$ and $b_m(x)$ are functional sequences defined by (7). But it can be shown easily that

$$\tilde{f}(x) = x^n A f(x),$$

where we have

$$\tilde{f}(x) = (b_1(x))^n f\left(\frac{a_1(x)}{b_1(x)}\right) = f_1(x).$$

Since $f_1(x)$ is a polynomial of degree $2n$, then

$$\begin{aligned} \tilde{f}_1(x) &= x^{2n} A(b_1(x))^n A f\left(\frac{a_1(x)}{b_1(x)}\right) \\ &= x^{2n}(Ab_1(x))^n f\left(\frac{Aa_1(x)}{Ab_1(x)}\right). \end{aligned} \tag{8}$$

From expression (8), in view of (7), we obtain

$$\tilde{f}_1(x) = (b_2(x))^n f\left(\frac{a_2(x)}{b_2(x)}\right) = f_2(x).$$

Consider now for any $m > 1$ the following relation:

$$f_m(x) = (b_m(x))^n f\left(\frac{a_m(x)}{b_m(x)}\right).$$

In this case

$$\tilde{f}_m(x) = x^{2^m n}(A(b_m(x)))^n A f\left(\frac{a_m(x)}{b_m(x)}\right).$$

Moreover, by (7) we have

$$\tilde{f}_m(x) = (b_{m+1}(x))^n f\left(\frac{a_{m+1}(x)}{b_{m+1}(x)}\right) = f_{m+1}(x),$$

which is the same as

$$f_{m+1}(x) = \sum_{u=0}^{n} c_u a_{m+1}^u(x) b_{m+1}^{n-u}(x).$$

The polynomial $\tilde{f}(x)$ is irreducible over $GF(2^s)$ by Theorem 1, if

$$\sum_{u=0}^{s-1} \left(\frac{c_1\delta}{c_0}\right)^{2^u} = 1. \tag{9}$$

Then it should be evident that in the polynomial

$$\tilde{f}(x) = \sum_{u=0}^{n} c_u(x^2 + \delta^2)^u x^{n-u} = \sum_{u=0}^{2n} h_u^{(1)} x^u = f_1(x)$$

the coefficients $h_{2n}^{(1)} = c_n = 1$, $h_0^{(1)} = c_n\delta^{2n} = \delta^{2n}$ and the coefficients for the 1st and $(2n-1)$th degrees of the variable are

$$h_1^{(1)} = c_{n-1}\delta^{2(n-1)}, \qquad h_{2n-1}^{(1)} = c_{n-1}.$$

It may be easily seen that for any m the coefficients in the polynomial

$$f_m(x) = \tilde{f}_{m-1}(x) = \sum_{u=0}^{2^m n} h_u^{(m)} x^u$$

are of the following form:

$$h_0^{(m)} = \delta^{2^m n}; \qquad h_1^{(m)} = c_{n-1}\delta^{2^m n - 2}; \qquad h_{2^m n-1}^{(m)} = c_{n-1}; \qquad h_{2^m n}^{(m)} = 1.$$

This property of the coefficients combined with the relation (9) leads us to the conclusion that for any m the polynomial

$$f_m(x) = \sum_{u=0}^{n} c_u a_m^u(x) b_m^{n-u}(x)$$

is irreducible over $GF(2^s)$, if

$$\sum_{u=0}^{s-1} \left(\frac{c_1\delta}{c_0}\right)^{2^u} = 1 \qquad \text{and} \qquad \sum_{u=0}^{s-1} \left(\frac{c_{n-1}}{\delta}\right)^{2^u} = 1.$$

Thus the following theorem holds.

THEOREM 3. *Let $\delta \neq 0$ be an element of $GF(2^s)$ and $f(x) = \sum_{u=0}^{n} c_u x^u$ be any irreducible polynomial over $GF(2^s)$ whose coefficients satisfy the conditions*

$$\sum_{u=0}^{s-1} \left(\frac{c_1\delta}{c_0}\right)^{2^u} = 1 \qquad \textit{and} \qquad \sum_{u=0}^{s-1} \left(\frac{c_{n-1}}{\delta}\right)^{2^u} = 1,$$

where $a_m(x)$ *and* $b_m(x)$ $(m > 1)$ *are sequences of functions defined by the recurrent equations*

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

under the initial conditions $a_1(x) = x^2 + \delta^2$ *and* $b_1(x) = x$. *Then the polynomial*

$$F(x) = \sum_{u=0}^{n} c_u a_m^u(x) b_m^{n-u}(x)$$

of degree $2^m n$ *is irreducible over* $GF(2^s)$.

For the case when $f(x) = x + a$ $(a \in GF(2^s),\ a \neq 0)$ we have the following corollaries.

COROLLARY 1. *The polynomial* $\varphi_m(x) = a_m(x) + ab_m(x)$ (*which is the same as* $\varphi_m(x) = x^{2^{m-1}} \varphi_{m-1}((x^2 + \delta^2)/x)$) *of degree* 2^m *is irreducible over* $GF(2^s)$ *if both the conditions*

$$\sum_{u=0}^{s-1} \left(\frac{\delta}{a}\right)^{2^u} = 1 \qquad \text{and} \qquad \sum_{u=0}^{s-1} \left(\frac{a}{\delta}\right)^{2^u} = 1$$

are satisfied.

COROLLARY 2. *Let* s *be an odd integer,* $\delta \neq 0$ *be any element of* $GF(2^s)$, *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 $\varphi_0 = x + \delta$. *Then, the polynomial* $\varphi_m(x)$ *of degree* 2^m *defined by the recurrent relation*

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

(*which is the same as*

$$\varphi_m(x) = \varphi_{m-1}^2(x) + \delta x \prod_{u=0}^{m-2} \varphi_u^2(x))$$

is irreducible over $GF(2^s)$.

Proof. From $\varphi_m(x) = a_m(x) + \delta b_m(x)$ we obtain

$$\varphi_m(x) = a_{m-1}^2(x) + (\delta b_{m-1}(x))^2 + \delta a_{m-1}(x) b_{m-1}(x) \tag{10}$$

and

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

By (7) we have that

$$b_{m-1}(x) = a_{m-2}(x) b_{m-2}(x) = a_{m-2}(x) a_{m-3}(x) b_{m-3}(x),$$

and hence

$$b_{m-1}(x) = a_{m-2}(x) a_{m-3}(x) \cdot \cdots \cdot a_1(x) b_1(x). \tag{11}$$

Substituting relation (11) in formula (10) and using the fact that $a_u(x) = \varphi_{u-1}^2(x)$ and $b_1(x) = x$, we obtain

$$\varphi_m(\mathrm{x}) = \varphi_{m-1}^2(x) + \delta x \prod_{u=0}^{m-2} \varphi_u^2(x).$$

But, according to Corollary 1, the polynomial $\varphi_m(x)$ is irreducible over $GF(2^s)$, since the conditions $a = \delta$ and the oddness of s imply that

$$\sum_{u=0}^{s-1} \left(\frac{\delta}{a}\right)^{2^u} = \sum_{u=0}^{s-1} 1 = 1 \qquad \text{and} \qquad \sum_{u=0}^{s-1} \left(\frac{a}{\delta}\right)^{2^u} = 1.$$

Thus Corollary 2 is proved. ■

In particular, for $s = 1$ this Corollary 2 matches with Theorem 5 given by Varshamov in [8].

It is easy to prove that for $\delta = 1$ the polynomial $\tilde{f}(x)$ is a self-dual polynomial. Indeed,

$$\tilde{f}^*(x) = x^{2n} \left(\frac{1}{x}\right)^n f\left[\frac{(1/x)^2 + 1}{1/x}\right] = x^n f\left(\frac{x^2+1}{x}\right) = \tilde{f}(x);$$

i.e., $\tilde{f}(x) = \tilde{f}^*(x)$, where $f^*(x) = x^n f(1/x)$. This fact plays an important role in the theory of the synthesis of irreducible self-dual polynomials and allows the construction of irreducible self-dual polynomials of high degrees over $GF(2^s)$ in explicit form.

Corollary 3. *Let $f(x)=\sum_{u=0}^{n} c_u x^u$ be an irreducible polynomial over $GF(2^s)$ whose coefficients satisfy the conditions*

$$\sum_{u=0}^{s-1}\left(\frac{c_1}{c_0}\right)^{2^u}=1 \qquad \textit{and} \qquad \sum_{u=0}^{s-1}(c_{n-1})^{2^u}=1.$$

Then, the self-dual polynomial

$$F(x)=\sum_{u=0}^{n} c_u a_m^u(x) b_m^{n-u}(x)$$

of degree $2^m n$ is irreducible over $GF(2^s)$.

For $s=1$ this corollary matches with Theorem 4 given by Varshamov in [7].

Notice that we have from Theorem 2 that $f(x)\neq\psi(x)$ for $p\neq 2$; i.e., a result analogous to the one in Theorem 3 is not valid for finite fields of odd characteristic.

Now we shall pass to the construction of irreducible polynomials. We will give later a method to construct irreducible polynomials of high degrees over $GF(2)$ in explicit form using Varshamov's results obtained in [8], thus continuing this work.

We start by introducing Varshamov's operator [8]

$$L^{\theta} f(x)=\frac{1}{\theta(x)}\sum_{u=0}^{n}\sum_{v=0}^{m} a_u\theta_v x^{vq^u},$$

where $f(x)=\sum_{u=0}^{n} a_u x^u$ and $\theta(x)=\sum_{v=0}^{m}\theta_v x^v$, $\quad a_u,\ \theta_v\in GF(q)$.

Let $\sum_\sigma=\{f_1(x), f_2(x),\ldots,f_\sigma(x)\}$ be a set of σ primitive polynomials with pairwise relatively prime degrees $n_1, n_2, n_3,\ldots,n_\sigma$ ($n_i>1$), respectively, over $GF(2)$; $T=\prod_{i=1}^{\sigma}(2^{n_i}-1)$; $\varphi(x)$ is an irreducible polynomial of degree n over $GF(2)$; $\gcd(n,T)=1$; G_σ is the selection of all possible sequences $\varepsilon=(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_\sigma)$ of length σ, where $\varepsilon_i=0$ or 1. Furthermore, let for any sequence $\varepsilon\in G_\sigma$

$$f(x,\varepsilon,\textstyle\sum_\sigma)=L^x\displaystyle\prod_{i=1}^{\sigma} f_i(x)^{\varepsilon_i},$$

$$xf(x,\varepsilon,\textstyle\sum_\sigma)\equiv R^{(\varepsilon)}(x)\ (\mathrm{mod}\ \varphi(x)),$$

and $\psi^{(\varepsilon)}(x) = \sum_{u=0}^{n} \psi_u^{(\varepsilon)} x^u$, where $\psi_u^{(\varepsilon)}$ is a nontrivial solution of the congruence

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

Then we have the following theorem.

THEOREM 4. *The polynomials*

$$F(x) = (\varphi(x))^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \mid (\sigma - |\varepsilon|)}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \sum_\sigma))}{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \nmid (\sigma - |\varepsilon|)}} \psi^{(\varepsilon)}(xf(x, \varepsilon, \sum_\sigma))} \tag{12}$$

and $\psi^{(v)}(x)$ of degree nT and n, respectively (*where $|\varepsilon| = \sum_{i=1}^{\sigma} \varepsilon_i$ and $v \in G_\sigma$*), *are irreducible over GF* (2).

Proof. *For* $n = 1$ the validity of the theorem follows directly from [8]. Therefore we prove the theorem for the case when $n > 1$. By [8], the polynomial

$$H(x) = \frac{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \mid (\sigma - |\varepsilon|)}} f(x, \varepsilon, \sum_\sigma)}{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \nmid (\sigma - |\varepsilon|)}} f(x, \varepsilon, \sum_\sigma)}$$

of degree T is irreducible over $GF(2)$. But gcd $(n, T) = 1$, and therefore $H(x)$ is also irreducible over $GF(2^n)$. Then it should be evident that

$$H(x) = x^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \mid (\sigma - |\varepsilon|)}} xf(x, \varepsilon, \sum_\sigma)}{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \nmid (\sigma - |\varepsilon|)}} xf(x, \varepsilon, \sum_\sigma)}.$$

Therefore, if α is the root of the equation $\varphi(\alpha) = 0$, then by [2] since $n > 1$, for the coefficients of the polynomial $H(x - \alpha) = h(x) = \sum_{u=0}^{T} h_u x^u$ we have that $\deg_2 (h_0, h_1, \ldots, h_{T-1}) = n$. Hence $h(x)$ is irreducible over $GF(2^n)$. Furthermore, since $h^{(v)}(x) = H(x - \alpha^{2^v}) = \sum_{u=0}^{T} h_u^{2^v} x^u$ then the polynomial $H_1(x) = \prod_{v=0}^{n-1} h^{(v)}(x)$ is irreducible over GF (2) by [2]. Hence

$$H_1(x) = \prod_{v=0}^{n-1} (x - \alpha^{2^v})^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \mid (\sigma - |\varepsilon|)}} (xf(x, \varepsilon, \sum_\sigma) - \beta_\varepsilon^{2^v})}{\prod_{\substack{\varepsilon \in G_\sigma \\ 2 \nmid (\sigma - |\varepsilon|)}} (xf(x, \varepsilon, \sum_\sigma) - \beta_\varepsilon^{2^v})},$$

where

$$f(x, \varepsilon, \textstyle\sum_\sigma) = \displaystyle\sum_{v=0}^{r_\varepsilon} b_v^{(\varepsilon)} x^{2^v}, \qquad \beta_\varepsilon = \sum_{v=0}^{r_\varepsilon} b_v^{(\varepsilon)} \alpha^{2^v}, \qquad \text{and} \qquad r_\varepsilon = \sum_{i=1}^{\sigma} \varepsilon_i n_i,$$

or

$$H_1(x) = \varphi(x)^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon\in G_\sigma \\ 2|(\sigma-|\varepsilon|)}} \prod_{v=0}^{n-1}(xf(x,\varepsilon,\sum_\sigma) - \beta_\varepsilon^{2^v})}{\prod_{\substack{\varepsilon\in G_\sigma \\ 2\nmid(\sigma-|\varepsilon|)}} \prod_{v=0}^{n-1}(xf(x,\varepsilon,\sum_\sigma) - \beta_\varepsilon^{2^v})}. \tag{13}$$

We show now that β_ε is a proper element of $GF(2^n)$ for any ε. Assume the contrary, namely that $\deg_2(\beta_\varepsilon) = d$, where d is a proper divisor of n. Let $\sum_k = \{f_{i_1}(x), f_{i_2}(x), \dots, f_{i_k}(x)\}$ be any subset of $\sum_\sigma$ containing k elements $f_{i_1}(x), f_{i_2}(x), \dots, f_{i_k}(x)$; then by [8], the polynomial

$$\lambda(x,\sum_k) = \frac{\prod_{\substack{\varepsilon\in G_k \\ 2|(k-|\varepsilon|)}} f(x,\varepsilon,\sum_k)}{\prod_{\substack{\varepsilon\in G_k \\ 2\nmid(k-|\varepsilon|)}} f(x,\varepsilon,\sum_k)}$$

of degree $T_k = \prod_{u=0}^{k}(2^{n_{i_u}} - 1)$ is irreducible over GF (2). Using the fact that $\gcd(L^x g_1(x), L^x g_2(x)) = L^x \gcd(g_1(x), g_2(x))$ along with the separability of the expression $f(x,\varepsilon,\sum_k)$ in [6], we find that

$$\gcd(\lambda(x,\sum_k), f(x,\varepsilon,\sum_\sigma)) = 1,$$

if $|\varepsilon| < k$, and $\gcd(\lambda(x,\sum_k), f(x,\varepsilon,\sum_\sigma)) = \lambda(x,\sum_k)$, if $\sum_k \subset \sum_{|\varepsilon|=t} = \{f_{j_1}(x), f_{j_2}(x), \dots, f_{j_t}(x)\}$.

There are exactly $c_{\sigma-k}^{t-k}$ subsets $\sum_{|\varepsilon|=t}$ containing $\sum_k$. This means that $\lambda(x,\sum_k)$ is a divisor of the polynomial $\prod_{|\varepsilon|=t} f(x,\varepsilon,\sum_\sigma)$ of multiplicity $c_{\sigma-k}^{t-k}$. Hence, if we set $\mu = \sum_{2|u} c_{\sigma-k}^u$ and $\mu_1 = \sum_{2\nmid u} c_{\sigma-k}^u$, then $\lambda(x,\sum_k)$ will be a divisor of the polynomials $\prod_{\substack{\varepsilon\in G_\sigma \\ 2\nmid(\sigma-|\varepsilon|)}} f(x,\varepsilon,\sum_\sigma)$ and $\prod_{\substack{\varepsilon\in G_\sigma \\ 2|(\sigma-|\varepsilon|)}} f(x,\varepsilon,\sum_\sigma)$ of multiplicity μ and μ_1, if σ is odd and μ_1 and μ, respectively, if σ is even. It follows from the factorization $(x-1)^{\sigma-k} = \sum_{u=0}^{\sigma-k} c_{\sigma-k}^u x^u$ that μ is the sum of the coefficients of the even degrees of x and μ_1 is the sum of the coefficients of odd degrees of x. Therefore $\mu - \mu_1 = (1-1)^{\sigma-k} = 0$. Hence $\lambda(x,\sum_k)$ occurs with the same multiplicity in $\prod_{\substack{\varepsilon\in G_\sigma \\ 2\nmid(\sigma-|\varepsilon|)}} f(x,\varepsilon,\sum_\sigma)$ and in $\prod_{\substack{\varepsilon\in G_\sigma \\ 2|(\sigma-|\varepsilon|)}} f(x,\varepsilon,\sum_\sigma)$ and hence with the multiplicity of zero in their quotient.

Now using the procedure described above, for any ε (for example $|\varepsilon| = t$ and $\varepsilon_{i_1} = \varepsilon_{i_{12}} = \varepsilon_{i_1} \cdots = \varepsilon_{i_t} = 1$), we obtain

$$\lambda(x,\sum_{|\varepsilon|=t}) = \frac{L^x \prod_{u=1}^{t} f_{i_u(x)}}{\prod_{k=1}^{t-1} \prod_{\sum_k \subset \sum_t} \lambda(x,\sum_k)},$$

where the polynomials $\lambda(x,\sum_{|\varepsilon|})$ and $\lambda(x,\sum_k)$ of degree $T_t = \prod_{u=1}^{t}(2^{n_{i_u}} - 1)$ and $T_k = \prod_{u=1}^{k}(2^{n_{i_{j_u}}} - 1)$, respectively, are irreducible over GF (2). Since $\gcd(n, T_t) = 1$ and $\gcd(n, T_k) = 1$, then the polynomials $\lambda(x,\sum_t)$ and $\lambda(x,\sum_k)$ will be also irreducible over GF (2^n). Then for the coefficients of the polynomials

$$\lambda(x-\alpha, \textstyle\sum_t) = \prod_{u=0}^{T_t} \lambda_u x^u,$$
$$\lambda(x-\alpha, \textstyle\sum_k) = \prod_{u=0}^{T_k} \lambda'_u x^u \tag{14}$$

by [2] since $n > 1$, we have that $\deg_2(\lambda_0, \lambda_1, \ldots, \lambda_{T_t}) = n$ and $\deg_2(\lambda'_0, \lambda'_1, \ldots, \lambda'_{T_k}) = n$ and the polynomials (14) are irreducible over $GF(2^n)$. Besides also using the following easily provable fact that

$$\lambda(x-\alpha^{2^v}, \textstyle\sum_t) = \prod_{u=0}^{T_t} \lambda_u^{2^v} x^u,$$

$$\lambda(x-\alpha^{2^v}, \textstyle\sum_k) = \prod_{u=0}^{T_k} \lambda_u'^{2^v} x^u,$$

we have by [8] that the polynomials

$$F_1(x, \textstyle\sum_t) = \prod_{u=0}^{n-1} \lambda(x-\alpha^{2^u}, \textstyle\sum_t),$$

$$F_1(x, \textstyle\sum_k) = \prod_{v=0}^{n-1} \lambda(x-\alpha^{2^v}, \textstyle\sum_k)$$

are irreducible over $GF(2)$. Hence we obtain

$$F_1(x, \textstyle\sum_t) = \frac{\prod_{v=0}^{n-1}(xL^x \prod_{u=1}^{t} f_{i_u(x)} - (\sum_{u=0}^{N} V_u \alpha^{2^u})^{2^v})}{\varphi(x) \prod_{k=0}^{t-1} \prod_{\sum_k \subset \sum_t} F_1(x, \sum_k)}, \tag{15}$$

where $xL^x \prod_{v=0}^{t} f_{i_v(x)} = \sum_{u=0}^{N} V_u x^{2^u}$ and $N = \sum_{u=1}^{t} n_{i_u}$. It should be noted here that, because of the separability of the polynomial $xL^x \prod_{v=0}^{t} f_{i_v}(x) - \sum_{u=0}^{N} V_u \alpha^{2^u}$, the polynomials $\lambda(x-\alpha, \sum_t)$ and $\lambda(x-\alpha, \sum_k)$ $(k < t)$ are different; this implies that for pairwise relative primes $n_1, n_2, \ldots, n_\sigma$ $(n_i > 1)$, the polynomials $F_1(x, \sum_t)$ and $F_1(x, \sum_k)$ $(k < t)$ are also different. Thus, if $\deg_2(\sum_{u=0}^{N} V_u \alpha^{2^u}) = d$, then

$$\prod_{v=0}^{n-1}\left(x - \left(\sum_{u=0}^{N} V_u \alpha^{2^u}\right)^{2^v}\right) = (\psi(x, \textstyle\sum_t))^M,$$

where $n = dM$ and $M > 1$. Hence, by (15) we have

$$F_1(x, \textstyle\sum_t) = \frac{\psi(xL^x \prod_{u=1}^{t} f_{i_u(x)}, \sum_t)^M}{\varphi(x) \prod_{k=1}^{t-1} \prod_{\sum_k \subset \sum_t} F_1(x, \sum_k)}.$$

But since the polynomials $\varphi(x)$ and $F_1(x, \sum_k)$ ($\sum_k \subset \sum_t$) are different and irreducible over $GF(2)$, we obtain that

$$F_1(x, \textstyle\sum_t) = \psi\left(xL^x \displaystyle\prod_{u=1}^{t} f_{i_u(x)}, \textstyle\sum_t\right)^{M-1} G(x),$$

which is impossible since $F_1(x, \sum_t)$ is irreducible over $GF(2)$.

Hence $M = 1$ and, for any ε, β_ε is a proper element $GF(2^n)$, which in its turn determines irreducibility of the polynomials $\psi^{(\varepsilon)}(x) = \prod_{u=0}^{n-1}(x - \beta_\varepsilon^{2^u})$ over $GF(2)$ for any ε. Thus, in view of (13) the polynomial (12) is irreducible over $GF(2)$.

It should now be clear that

$$\psi^{(\varepsilon)}(R^{(\varepsilon)}(x)) \equiv 0 \pmod{\varphi(x)}$$

or

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

Thus the theorem is proved. ■

In exactly the same way as in Theorem 1 we can prove the following fact.

THEOREM 5. *Let* $\delta \in \{0, 1, 2\}$ $\gcd(n, 2^\delta \prod_{i=1}^{\sigma}(2^{n_i} - 1)) = 1$;

$$\theta(x) = xL^x(x+1)^\delta + 1;$$

$$f(\theta, \varepsilon, \textstyle\sum_\sigma) = \theta(x)L^\theta \displaystyle\prod_{i=1}^{\sigma} f_i(x)^{\varepsilon_i};$$

$$(\theta(x) + 1)L^{\theta+1} \prod_{i=1}^{\sigma} f_i(x)^{\varepsilon_i} \equiv R^{(\varepsilon)}(x) \pmod{\varphi(x)};$$

$$\theta(x) + 1 \equiv W(x) \pmod{\varphi(x)};$$

$$\psi^{(\varepsilon)}(x) = \sum_{u=0}^{n} \psi_u^{(\varepsilon)} x^u, \qquad \textit{and} \quad \omega(x) = \sum_{u=0}^{n} \omega_u x^u;$$

where $\psi_u^{(\varepsilon)}$ and ω_u are nontrivial solutions of the congruences

$$\sum_{u=0}^{n} \psi_u^{(\varepsilon)}(R^{(\varepsilon)}(x))^u \equiv 0 \,(\mathrm{mod}\, \varphi(x))$$

and

$$\sum_{u=0}^{n} \omega_u(W(x))^u \equiv 0 \,(\mathrm{mod}\, \varphi(x)),$$

respectively. Then the polynomials $\psi^{(v)}(x)$, $\omega(x)$ of degree n and the polynomial

$$F(x) = (\omega(\theta(x)))^{(-1)^\sigma} \frac{\prod_{\substack{\varepsilon\in G_\sigma \\ 2|(\sigma-|\varepsilon|)}} \psi^{(\varepsilon)}(f(\theta, \varepsilon, \sum_\sigma))}{\prod_{\substack{\varepsilon\in G_\sigma \\ 2\nmid(\sigma-|\varepsilon|)}} \psi^{(\varepsilon)}(f(\theta, \varepsilon, \sum_\sigma))}$$

of degree $2^\delta nT$ are irreducible over $GF(2)$.

Remark. It follows from [9] and [3] that if the following two conditions hold,

$$gcd(nr, q^m - 1) = 1, \qquad g(x) = \sum_{v=0}^{m} b_v x^v (g(x) \neq x - 1),$$

where $g(x)$ is a primitive polynomial over $GF(q)$, $f(x) = \sum_{u=0}^{n} a_u x^u$ is an irreducible polynomial over $GF(q^r)$,

$$\sigma_q^x(g(x), 0) = \sum_{u=0}^{n} a_u \left(\sum_{v=0}^{m} b_v x^{q^v} \right)^u \equiv R(x) (\mathrm{mod}\, f(x)),$$

and $\psi(x) = \sum_{u=0}^{n} \psi_u x^u$, where ψ_u is a nontrivial solution of the congruence

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

then the polynomials $\psi(x)$ and $F(x) = (f(x))^{-1}\sigma_q^{\psi}(g(x), 0)$ of degree n and $n(q^m - 1)$, respectively, are irreducible over $GF(q^r)$.

It is evident now that based on the above remark we may construct a polynomial $F(x)$ of degree $nT(T = \prod_{i=1}^{\sigma}(2^{n_i} - 1), \mathrm{gcd}(n, T) = 1)$ irreducible over $GF(2)$ wherever the conditions of Theorem 4 are satisfied.

Thus to construct $F(x)$ the polynomials $F_1(x), F_2(x), \dots, F_\sigma(x) = F(x)$ are constructed successively. $F_1(x)$ of degree $n(2^{n_1} - 1)$ is constructed by means of the polynomials $\varphi(x)$ and $f_1(x)$ (see Theorem 4). $F_2(x)$ is constructed with the help of $F_1(x)$ and the primitive polynomial $f_2(x), \dots, F_\sigma(x)$ using $F_{\sigma-1}(x)$ and

$f_\sigma(x)$. Moreover, at the jth ($j \leq \sigma$) construction step, a set of $n\prod_{i=1}^{j-1}(2^{n_i}-1)$ equations in $n\prod_{i=1}^{j-1}(2^{n_i}-1)$ unknowns is being solved.

Unlike the method described above, Theorems 4 and 5 allow us to construct an irreducible polynomial $F(x)$ of degree nT by solving directly only 2^σ systems each of n equations in n unknowns.

It is worth noting here that Theorems 4 and 5 are only valid over $GF(2)$.

ACKNOWLEDGMENTS

The author thanks Professor R. Varshamov for his helpful comments and suggestions made while working over this paper. I also thank the anonymous referees for a careful reading of my manuscript and for their very detailed comments. Their many helpful suggestions and corrections allowed me to improve the paper significantly.

REFERENCES

1. A. A. Albert, "Fundamental Concepts of Higher Algebra," University of Chicago Press, 1956.
2. M. K. Kyuregyan, On a method for constructing irreducible polynomials over Galois fields, *Dokl. Akad. Nauk Arm. SSR* **83** (1986), 58–61. [In Russian]
3. M. K. Kyuregyan, Permutations of Varshamov operator over Galois fields and their applications, *Dokl. Akad. Nauk Arm. SSR* **84** (1987), 159–163. [In Russian]
4. R. Peice and P. Egreen, "Communication Technique for Multipath Channels," Prac. 46, 1958.
5. S. Shwarz, On a class of polynomials over finite fields, *Mat.-fyzik. casopis SAV* **10** (1960), 68–80.
6. R. R. Varshamov, On a method for constructing irreducible polynomials over finite fields, *Dokl. Akad. Nauk Arm. SSR* **79** (1984), 26–28. [In Russian]
7. R. R. Varshamov, A general method for constructing irreducible polynomials over Galois fields, *Dokl. Akad. Nauk SSSR* **275** (1984), 1041–1044. [In Russian]
8. R. R. Varshamov, On a theorem from the theory of irreducibility of polynomials, *Dokl. Akad. Nauk SSSR* **156** (1964), 1308–1311. [In Russian]
9. R. R. Varshamov, Operator permutations over Galois fields, *Dokl. Akad. Nauk SSSR* **221** (1973), 768–771. [In Russian]
10. N. Zierler, Linear recurring sequences, *J. Soc. Induct. Appl. Math.* **7** (1959), 31–48.
11. R. Lidl and H. Niederreiter, Finite fields, *in* "Encyclopedia of Mathematics and Its Applications: Algebra," Vol. 20, Addison-Wesley, London/Amsterdam, Don Mills, Ontario/Sydney/Tokyo, 1983.
12. S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, *Designs, Codes Cryptogr.* **2** (1992), 169–174.
13. A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, "Applications of Finite Fields," Chap. 3, Kluwer Academic Boston/Dordrecht/Lancaster, 1993.