Mathematica Slovaca

Štefan Schwarz

Irreducible polynomials over finite fields with linearly independent roots

*Mathematica Slovaca*, Vol. 38 (1988), No. 2, 147--158

Persistent URL: `http://dml.cz/dmlcz/136468`

**Terms of use:**

© Mathematical Institute of the Slovak Academy of Sciences, 1988

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://project.dml.cz`

Math. Slovaca 38, 1988, No. 2, 147—158

# IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS WITH LINEARLY INDEPENDENT ROOTS

ŠTEFAN SCHWARZ

Let $GF(q) = F_q$ be a finite field, $q = p^s$, $s \geqq 1$, $p$ a prime. Let $f(x)$ be a monic irreducible polynomial of degree $n$ over $F_q$ and $\alpha$ a root of $f(x) = 0$. If $\beta$ is an element of the field $F_q(\alpha)$ and the elements $\beta, \beta^q, \ldots, \beta^{q^{n-1}}$ are linearly independent over $F_q$, then the set $\Omega = \{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ is called a normal basis of $F_q(\alpha)$ over $F_q$, and $\beta$ is called a generator of the normal basis $\Omega$. It is well known that such a basis always exists, and any element of $\Omega$ is a generator of $\Omega$.

It is known that $F_q(\alpha)$ is a cyclic extension of $F_q$ with the (cyclic) Galois group $G$ of order $n$. The automorphism $x \to x^q$ is a generator of $G$.

The problem to be discussed in this paper is the following. Given a fixed chosen monic irreducible polynomial $f(x)$ of degree $n$ over $F_q$ we have to decide whether the roots of $f(x) = 0$ represent a normal basis of $F_q(\alpha)$ over $F_q$. For convenience we shall call a polynomial having this property an N-polynomial.

There is a straightforward way how to verify whether a given polynomial is an N-polynomial or not. We represent the roots $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ of $f(x) = 0$ as polynomials of degree at most $n - 1$ in $\alpha$:

$$\alpha^{q^i} = b_{i0} + b_{i1}\alpha + \ldots + b_{i,n-1}\alpha^{n-1}, \quad (i = 0, 1, \ldots, n-1).$$

[Hereby $b_{01} = 1$, $b_{00} = b_{02} = \ldots = b_{0,n-1} = 0$.]
If the $n \times n$ matrix $B = (b_{ij})$ is non-singular, then $f(x)$ is an N-polynomial. If $n$ is small, we can establish directly whether $B$ is non-singular. However, if $n$ is large (say $n \geqq 10$), this method may require a great number of computations.

In this paper we present a method how to avoid the consideration of large matrices. The result obtained is a wide generalization of that given in the paper [4], and the proofs, as well as the results, are different. In [4] the authors deal only with the field $F_2$, while the result of the present paper holds for any finite field. [Of course $F_2$ is the most important case for the coding theory.] Also the authors of [4] (as well as the paper [5], which has a different main aim) deal only with the case that $n = 2^u \cdot r^v$, where $r$ is a prime, while in the present paper $n$ may be any positive integer.

Our method is based on a statement proved in [9] which holds for cyclic extensions of any field. In order to make the present paper independent of [9], I give here a direct proof of this statement for finite fields (see Lemma 1). This is then used to prove the main result.

## 1. The Theorem

We retain the notations introduced above and introduce the matrix $C = (c_{ij})$ defined by

$$\begin{aligned} 1 &= c_{00} + c_{01}\alpha + c_{02}\alpha^2 + \dots + c_{0,n-1}\alpha^{n-1}, \\ \alpha^q &= c_{10} + c_{11}\alpha + c_{12}\alpha^2 + \dots + c_{1,n-1}\alpha^{n-1}, \\ \alpha^{2q} &= c_{20} + c_{21}\alpha + c_{22}\alpha^2 + \dots + c_{2,n-1}\alpha^{n-1}, \\ &\vdots \\ \alpha^{(n-1)q} &= c_{n-1,0} + c_{n-1,1}\alpha + c_{n-1,2}\alpha^2 + \dots + c_{n-1,n-1}\alpha^{n-1}. \end{aligned} \tag{1}$$

[Here $c_{00} = 1, \quad c_{01} = \dots = c_{0,n-1} = 0$.]
Denote $A = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})^T$ (where $T$ denotes the transpose). The identities (1) can be written in the form

$$[1, \alpha^q, \alpha^{2q}, \dots, \alpha^{(n-1)q}]^T = C \cdot A.$$

If $f(x)$ is irreducible (over $F_q$) (as we supposed), it is known (see [8]) that $C$ is non-singular and $\lambda^n - 1$ is the minimal polynomial of the matrix $C$. [As a matter of fact it can be proved that $\det|C| = (-1)^{n-1}$, but this is irrelevant for our purposes.]

If $\beta = r_0 + r_1\alpha + \dots + r_{n-1}\alpha^{n-1} = (r_0, r_1, \dots, r_{n-1})A$, $(r_i \in F_q)$, we have $\beta^q = (r_0, r_1, \dots, r_{n-1})\ [1, \alpha^q, \alpha^{2q}, \dots, \alpha^{(n-1)q}]^T = (r_0, r_1, \dots, r_{n-1})CA$. Further $\beta^{q^2} = (r_0, r_1, \dots, r_{n-1})C^2A$, and, in general, we have

$$\beta^{q^i} = (r_0, r_1, \dots, r_{n-1})C^i \cdot A \quad \text{for} \quad i = 0, 1, 2, \dots, n-1.$$

(Note that $C^n = E$, where $E$ is the $n \times n$ unit matrix.)

Denote $\varrho = (r_0, r_1, \dots, r_{n-1})$, then

$$(\beta, \beta^q, \beta^{q^2}, \dots, \beta^{q^{n-1}})^T = \begin{pmatrix} \varrho \\ \varrho C \\ \varrho C^2 \\ \vdots \\ \varrho C^{n-1} \end{pmatrix} \cdot A.$$

Hence the set $(\beta, \beta^q, \ldots, \beta^{q^{n-1}})$ is a normal basis if and only if the matrix $Q = \begin{pmatrix} \varrho \\ \varrho C \\ \vdots \\ \varrho C^{n-1} \end{pmatrix}$ is non-singular.

For any vector $\varrho$ we have $\varrho C^n = \varrho$, i.e. $\varrho(C^n - E) = \bar{0}$ (the zero row vector). Denote by $\psi_\varrho(\lambda)$ the monic $\lambda$-polynomial of smallest degree (with coefficients in $F_q$) such that $\varrho \cdot \psi_\varrho(C) = \bar{0}$. Clearly the degree of $\psi_\varrho(C)$ is $\leqq n$. (The polynomial $\psi_\varrho(\lambda)$ is called the minimal polynomial of $\varrho$ with respect to $C$.) It is known that $\psi_\varrho(\lambda)$ is uniquely determined and $\psi_\varrho(\lambda)$ divides $\lambda^n - 1$.

The condition $\det|Q| \neq 0$ says that the minimal polynomial of $\varrho$ (with respect to $C$) is $\lambda^n - 1$. Decompose $\lambda^n - 1$ into the product of monic irreducible factors over $F_q$. This factorization is of the form

$$\lambda^n - 1 = [\varphi_1(\lambda) \ldots \varphi_r(\lambda)]^t,$$

where $t = 1$ if $(n,p) = 1$, and $t = p^e$ if $n = m \cdot p^e$, $(n,m) = 1$. Denote the degree of $\varphi_i(\lambda)$ by $d_i$. Construct the polynomials $\Phi_i(\lambda) = \dfrac{\lambda^n - 1}{\varphi_i(\lambda)}$ of degree $n - d_i$. The minimal polynomial of $\varrho$ (with respect to $C$) is $\lambda^n - 1$ if and only if $\varrho \cdot \Phi_i(C) \neq 0$ for $i = 1, 2, \ldots, r$. We have proved the following.

**Lemma 1.** *An element $\beta = \varrho \cdot A \in F_q(\alpha)$ is a generator of a normal basis if and only if $\varrho$. $\Phi_i(C) \neq \bar{0}$ for $i = 1, 2, \ldots, r$.*

We now return to the original problem, namely to find under what conditions $\alpha$ itself [i.e. the root of the given $f(x)$] is a generator of a normal basis (i.e., $f(x)$ is an N-polynomial). Now $\alpha = (0, 1, 0, 0, \ldots, 0) \cdot A$. Hence $f(x)$ is an N-polynomial if and only if $(0, 1, 0, \ldots, 0)\, \Phi_i(C) \neq (0, 0, \ldots, 0)$, for $i = 1, \ldots, r$, i.e.,

$$(0, 1, 0, 0, \ldots, 0)\, \Phi_i(C) \cdot A \neq \bar{0}. \tag{2}$$

Assume $\Phi_i(\lambda) = b_0^{(i)} + b_1^{(i)}\lambda + b_2^{(i)}\lambda^2 + \ldots + b_{n-d_i-1}^{(i)}\lambda^{n-d_i-1} + \lambda^{n-d_i}$.

*Clearly* $(0, 1, 0, \ldots, 0)\, \Phi_i(C)\, A$ is equal to the second term of the column vector $\Phi_i(C) \cdot A$. Now the second term of $E \cdot A$ is $\alpha$, the second term of $C \cdot A$ is $\alpha^q$, and, in general, the second term of $C^j A$ is $\alpha^{q^j}$ $(j = 0, 1, \ldots, n-1)$. Hence the second term of $\Phi_i(C)\, A$ is

$$b_0^{(i)}\alpha + b_1^{(i)}\alpha^q + b_2^{(i)}\alpha^{q^2} + \ldots + b_{n-d_i-1}^{(i)}\alpha^{q^{n-d_i-1}} + \alpha^{q^{n-d_i}}.$$

We have proved the following

**Theorem.** *Let $f(x)$ be a monic irreducible polynomial of degree $n$ over $F_q$ and $\alpha$ a root of $f(x) = 0$. Let $\lambda^n - 1 = [\varphi_1(\lambda) \ldots \varphi_r(\lambda)]^t$, $t \geqq 1$, be the factorization of $\lambda^n - 1$ into monic irreducible polynomials over $F_q$. Denote*

$$\Phi_i(\lambda) = \frac{\lambda^n - 1}{\varphi_i(\lambda)} = b_0^{(i)} + b_1^{(i)}\lambda + b_2^{(i)}\lambda^2 + \dots + b_{n-d_i-1}^{(i)}\lambda^{n-d_i-1} + \lambda^{n-d_i}. \tag{3}$$

*Then $\alpha$ is a generator of a normal basis of $F_q(\alpha)$ over $F_q$ if and only if for $i = 1, 2, \dots, r$, we have*

$$b_0^{(i)}\alpha + b_1^{(i)}\alpha^q + b_2^{(i)}\alpha^{q^2} + \dots + b_{n-d_i-1}^{(i)}\alpha^{q^{n-d_i-1}} + \alpha^{q^{n-d_i}} \neq 0. \tag{4}$$

Notation, If $\Phi_i(\lambda)$ is the polynomial (3), we shall denote the left hand side of (4) by $\hat{\Phi}_i(\alpha)$. [Clearly $\hat{\Phi}_i(\lambda)$ is a $q$-polynomial of Ore, often called also the linearized polynomial of $\Phi_i(\lambda)$. See [2].] The linearized polynomials appear here in an quite natural way. No knowledge about their properties is needed in what follows.

Remark 1. Since $\lambda - 1$ is always a factor of $\lambda^n - 1$ one of the $r$ conditions is always $\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{n-1}} \neq 0$.

Remark 2. Ore ([3]) proved that the number $\nu$ of N-polynomials of degree $n$ over $F_q$ is given by the formula

$$\nu = \frac{1}{n} q^n (1 - q^{-d_1})(1 - q^{-d_2}) \dots (1 - q^{-d_r}).$$

Remark 3. Peterson and Weldon ([6]) list the set of all N-polynomials over $F_2$ of degree $n \leqq 16$ and some N-polynomials of degree $17 \leqq n \leqq 34$. As far as I can decide analogous tables, e.g., for $F_3$ have not been published. (See however [1].)

## 2. Examples

We first recall some known results concerning the decomposition of

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + 1) \tag{5}$$

over $F_q$ into irreducible factors.

Let $\sigma_k$ be the number of monic irreducible factors of $x^n - 1$ of degree $k$ over $F_q$. If $(n, q) = 1$, it is known (see [7]) that

$$\sigma_k = \frac{1}{k} \sum_{t|k} \mu\left(\frac{k}{t}\right)(n, q^k - 1), \qquad (k = 1, 2, \dots, n),$$

where $\mu$ is the Moebius function. Otherwise stated the numbers $\sigma_k$ may be successively calculated from the system of linear equations

$$\sum_{t|k} t\sigma_k = (n, q^k - 1), \qquad k = 1, 2, \dots, \left[\frac{n}{2}\right].$$

(See Example 4 below.)

The following Corollaries of this general formula will be freely used in the sequel.

a) If $n > 2$ is a prime, and $q$ belongs $(\bmod n)$ to the exponent $l$, then the second factor on the right-hand side in (5) is a product of $\frac{n-1}{l}$ irreducible factors of degree $l$ (over $F_q$).

b) Let $r$ be a prime, $(r, q) = 1$ and denote $Q_{r^i}(x) = (x^{r^i} - 1)/(x^{r^{i-1}} - 1)$. Let $n = r^v$, $v \geqq 1$. If $q$ is a primitive element $(\bmod n)$, then each factor in the decomposition

$$x^n - 1 = (x - 1) \cdot Q_r(x) \cdot Q_{r^2}(x) \dots Q_{r^v}(x)$$

is irreducible over $F_q$.

Example 1. The simplest case is the following. Let $f(x) = x^n + a_1 \cdot x^{n-1} + \dots + a_n$ be an irreducible polynomial of degree $n = p^e$ over $F_q = GF(p^s)$ and $\alpha$ a root of $f(x) = 0$.

In this case $x^n - 1 = (x - 1)^{p^e}$. Hence $\Phi(x) = 1 + x + x^2 + \dots + x^{n-1}$, and $\hat{\Phi}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{n-1}} = \mathrm{Tr}(\alpha) = -a_1$. Hence our polynomial is an N-polynomial if and only if $\mathrm{Tr}(\alpha) = -a_1 \neq 0$.

This is a known result going back at least to [5].

Example 2. Let $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ be an irreducible polynomial over $F_p$ and $n$ a prime, $(n, p) = 1$. Suppose moreover that $p$ is a primitive element $(\bmod n)$. We have to decide under what conditions $f(x)$ is an N-polynomial (over $F_p$).

In this case $\Phi_1(\lambda) = \lambda - 1$, $\Phi_2(\lambda) = 1 + \lambda + \dots + \lambda^{n-1}$. Denoting by $\alpha$ a root of $f(x) = 0$ we have as necessary and sufficient conditions: a) $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \dots + \alpha^{p^{n-1}} = -a_1 \neq 0$, and b) $\alpha^p - \alpha \neq 0$.

The second condition is certainly satisfied since the roots $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}}$ of an irreducible polynomial are all different.

Hence we have the result: If $n$ is prime and $p$ is a primitive element $(\bmod n)$, then $f(x)$ is an N-polynomial over $F_p$ if and only if $\mathrm{Tr}(\alpha) = -a_1 \neq 0$.

Consider, e.g., the field $F_2$. The number $p = 2$ is a primitive element mod 3, 5, 11, 13, 19, .... Hence over the field $F_2$ the irreducible polynomials of degree 3, 5, 11, 13, 19, ... are N-polynomials if and only if $\mathrm{Tr}(\alpha) \neq 0$, i.e. $a_1 = 1$.

Consider next the field $F_3$. The number $p = 3$ is a primitive element mod 5, 7, 17, 19, .... hence, over the field $F_3$ the monic irreducible polynomials of degree 5, 7, 17, 19, ... are N-polynomials if and only if $\mathrm{Tr}(\alpha) \neq 0$, i.e. $a_1 = 1$ or $a_1 = 2$.

Example 3. Consider the field $F_2$ and suppose again that $n$ is a prime.

The number $p = 2$ is not a primitive element mod 7, 17, 23, 31, ..., so that in these cases the second term on the right hand side of (5) is not irreducible over $F_2$.

A) For $n = 7$ we have

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1).$$

Hence $\Phi_1(\lambda) = 1 + \lambda + \lambda^2 + \ldots + \lambda^6$, $\Phi_2(\lambda) = 1 + \lambda + \lambda^2 + \lambda^4$, $\Phi_3(\lambda) = 1 + \lambda^2 + \lambda^3 + \lambda^4$.

Hence a polynomial of degree 7 over $F_2$ is an N-polynomial if and only if the following three conditions are satisfied:

a) $\mathrm{Tr}(\alpha) = a_1 = 1$.

b) $\hat{\Phi}_2(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \alpha^{2^4} = \alpha + \alpha^2 + \alpha^4 + \alpha^{16} \neq 0$.

c) $\hat{\Phi}_3(\alpha) = \alpha + \alpha^{2^2} + \alpha^{2^3} + \alpha^{2^4} = \alpha + \alpha^4 + \alpha^8 + \alpha^{16} \neq 0$.

(Note, by the way, that there exist 18 irreducible polynomials of degree 7 over $F_2$, 7 of them being N-polynomials.)

B) To see how this works, consider a concrete irreducible polynomial over $F_2$, e.g., $f(x) = x^7 + x^6 + x^4 + x^2 + 1$. If $f(\alpha) = 0$, we have by successive multiplication (in such a simple case by hand computations):

$$\alpha^7 = 1 + \alpha^2 + \alpha^4 + \alpha^6, \qquad \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^5,$$
$$\alpha^8 = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6, \qquad \alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6.$$
$$\alpha^{10} = \alpha + \alpha^2 + \alpha^4 + \alpha^6,$$

Hence:

$$\hat{\Phi}_2(\alpha) = \alpha + \alpha^2 + \alpha^4 + (1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6) = 1 + \alpha^2 + \alpha^3 + \alpha^6 \neq 0,$$

$$\hat{\Phi}_3(\alpha) = \alpha + \alpha^4 + (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6) + (1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6) = \\ = \alpha + \alpha^2 + \alpha^4 + \alpha^5 \neq 0.$$

All the three conditions are satisfied, hence our polynomial is an N-polynomial.

C) In this simple case we can write down the $7 \times 7$ matrix corresponding to the straightforward method mentioned at the beginning. We need $\alpha^{32} = 1 + \alpha^2 + \alpha^3 + \alpha^4$, $\alpha^{64} = \alpha + \alpha^2 + \alpha^3 + \alpha^5$. Then the matrix (formed by the coefficients of $\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{64}$)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

is easily seen to have the determinant equal to 1 (in $F_2$).

D) The advantage of our method becomes clear if $n$ is large. Consider the case of a polynomial of degree 17 over $F_2$. Since $p = 2$ belongs to exponent 8 (mod 17), the second term in (5) is a product of two irreducible factors of degree 8. The corresponding factorization is

$$x^{17} - 1 = (1 + x)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x^3 + x^4 + x^5 + x^8).$$

This implies:

$$\Phi_1(\lambda) = \sum_{i=0}^{16} \lambda^i,$$

$$\Phi_2(\lambda) = 1 + \lambda + \lambda^3 + \lambda^6 + \lambda^9,$$

$$\Phi_3(\lambda) = 1 + \lambda^3 + \lambda^4 + \lambda^6 + \lambda^9,$$

Hence an irreducible polynomial of degree 17 over $F_2$ is an N-polynomial if and only if

a) $\mathrm{Tr}(\alpha) = a_1 = 1$,
b) $\alpha + \alpha^2 + \alpha^8 + \alpha^{64} + \alpha^{512} \neq 0$,
c) $\alpha + \alpha^8 + \alpha^{16} + \alpha^{64} + \alpha^{512} \neq 0$.

This is, of course, essentially simpler than to deal with a $17 \times 17$ matrix.

Example 4. Consider again $F_2$ and an irreducible polynomial $f(x)$ of (composite) degree 21.

To find the degrees of the irreducible factors of $x^{21} - 1$, we consider the system of equations:

$$\sigma_1 = (21, 2 - 1), \qquad 4\sigma_4 + 2\sigma_2 + \sigma_1 = (21, 2^4 - 1),$$

$$2\sigma_2 + \sigma_1 = (21, 2^2 - 1), \qquad 5\sigma_5 + \sigma_1 = (21, 2^5 - 1),$$

$$3\sigma_3 + \sigma_1 = (21, 2^3 - 1), \quad 6\sigma_6 + 3\sigma_3 + 2\sigma_2 + \sigma_1 = (21, 2^6 - 1).$$

This gives immediately $\sigma_1 = 1$, $\sigma_2 = 1$, $\sigma_3 = 2$, $\sigma_4 = 0$, $\sigma_5 = 0$, $\sigma_6 = 2$, i.e. there is one linear factor, one quadratic factor, two factors of degree 3 and two factors of degree 6.

The factorization itself is

$$x^{21} - 1 = (1 + x)(1 + x + x^2)(1 + x + x^3)(1 + x^2 + x^3).$$
$$(1 + x + x^2 + x^4 + x^6)(1 + x^2 + x^4 + x^5 + x^6).$$

This implies:

$$\Phi_1(\lambda) = \sum_{i=0}^{20} \lambda^i,$$

$$\Phi_2(\lambda) = \sum_{u \in U_2} \lambda^u, \quad U_2 = \{0, 1, 3, 4, 6, 7, 10, 12, 13, 15, 16, 18, 19\}.$$

$$\Phi_3(\lambda) = \sum_{u \in U_3} \lambda^u, \quad U_3 = \{0, 1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18\}.$$

$$\Phi_4(\lambda) = \sum_{u \in U_4} \lambda^u, \quad U_4 = \{0, 2, 3, 4, 7, 9, 10, 11, 14, 16, 17, 18\}.$$

$$\Phi_5(\lambda) = \sum_{u \in U_5} \lambda^u, \quad U_5 = \{0, 1, 3, 6, 7, 10, 13, 15\}.$$

$$\Phi_6(\lambda) = \sum_{u \in U_6} \lambda^u, \quad U_6 = \{0, 2, 5, 8, 9, 12, 14, 15\}.$$

Define $\alpha$ by $f(\alpha) = 0$. We have the following result:

The polynomial $f(x)$ is an N-polynomial if and only if the following 6 conditions are satisfied: $\mathrm{Tr}(\alpha) = a_1 = 1$, $\hat{\Phi}_i(\alpha) \neq 0$ $(i = 2, 3, \ldots, 6)$.

Remark. If $\mathrm{Tr}(\alpha) = 1$, then we may replace, e.g., the second condition by $1 + \sum_{u \in \bar{U}_2} \alpha^{2^u} \neq 0$, where $\bar{U}_2 = \{2, 5, 8, 9, 11, 14, 17, 20\}$.

In examples of this type machine computation is inevitable. Note also: Since $n > 16$ the tables in [6] cannot help in this case. Note finally that there exist 99858 monic irreducible polynomials of degree 21 over $F_2$. 27783 of them are N-polynomials. This should emphasize that there are some reasonable limits for the construction of tables.

Example 5. Consider the field $F_3$ and an irreducible polynomial $f(x)$ of degree 25 over $F_3$.

Since $p = 3$ is a primitive element (mod $5^2$), we have

$$x^{25} - 1 = (x - 1)\cdot Q_5(x)\cdot Q_{25}(x) = (x - 1)(x^4 + x^3 + x^2 + x + 1)\cdot \\ \cdot(x^{20} + x^{15} + x^{10} + x^5 + 1),$$

where the polynomials to the right are irreducible over $F_3$. We have

$$\Phi_1(\lambda) = \sum_{i=0}^{24} \lambda^i,$$

$$\Phi_2(\lambda) = -1 + \lambda - \lambda^5 + \lambda^6 - \lambda^{10} + \lambda^{11} - \lambda^{15} + \lambda^{16} - \lambda^{20} + \lambda^{21},$$

$$\Phi_3(\lambda) = \lambda^5 - 1.$$

Define $\alpha$ by $f(\alpha) = 0$, and denote $S(\lambda) = 1 + \lambda^5 + \lambda^{10} + \lambda^{15} + \lambda^{20}$. We have $\hat{\Phi}_1(\alpha) = \mathrm{Tr}(\alpha)$.

$$\hat{\Phi}_2(\alpha) = -[\alpha + \alpha^{3^5} + \alpha^{3^{10}} + \alpha^{3^{15}} + \alpha^{3^{20}}] + [\alpha^3 + \alpha^{3^6} + \alpha^{3^{11}} + \alpha^{3^{16}} + \alpha^{3^{21}} =$$
$$= -[\hat{S}(\alpha)] + [\hat{S}(\alpha)]^3 = \hat{S}(\alpha)\cdot[\hat{S}\alpha) - 1]\cdot[\hat{S}(\alpha) - 2].$$
$$\hat{\Phi}_3(\alpha) = \alpha^{3^5} - \alpha.$$

$\hat{\Phi}_3(\alpha) \neq 0$ is certainly satisfied since the roots of our irreducible polynomial $\alpha, \alpha^3, \alpha^{3^2}, \ldots, \alpha^{3^{24}}$ are all different.

We have the following result: An irreducible polynomial of degree 25 over $F_3$ is an N-polynomial if and only if

a) $\mathrm{Tr}(\alpha) \neq 0$.

b) The element $\alpha + \alpha^{3^5} + \alpha^{3^{10}} + \alpha^{3^{15}} + \alpha^{3^{20}}$ is not an element of the ground field $F_3$ (i.e. 0, 1, 2).

Before proceeding to the next examples we prove the following simple

**Lemma 2.** *Let $f(x)$ be an irreducible polynomial of degree $n$ over $F_2$ and $f(\alpha) = 0$. Let $t$ be a divisor of $n$ and $s = n/t$. Denote*

$$S(t, \alpha) = \sum_{u \in U_t} \alpha^{2^u}, \quad \textit{where} \quad U_t = \{0, t, 2t, \ldots, (s-1)\,t\}.$$

*If* $\mathrm{Tr}(\alpha) = 1$, *then* $S(t, \alpha) \neq 0$.

Proof. For any non-negative integer $v$ we have $[S(t,\alpha)]^{2^v} = \sum_{u \in U_t} \alpha^{2^{u+v}} = \sum_{u \in U_{t,v}} \alpha^{2^u}$, where $U_{t,v} = \{v, t+v, \ldots, (s-1)\,t+v\}$. If $v$ runs through $\{0, 1, 2, \ldots, t-1\}$, we have

$$U_t \cup U_{t,1} \cup \ldots \cup U_{t,t-1} = \{0, 1, 2, \ldots, n-1\}.$$

Hence

$$\mathrm{Tr}(\alpha) = S(t,\alpha) + [S(t,\alpha)]^2 + [S(t,\alpha)]^{2^2} + \ldots + [S(t,\alpha)]^{2^{t-1}}.$$

Now $S(t, \alpha) = 0$ would imply $\mathrm{Tr}(\alpha) = 0$, contrary to our assumption.

Example 6. Let $n = 2^k \cdot r$, where $k \geqq 1$, $r > 2$ a prime, and suppose that 2 is a primitive element $(\mathrm{mod}\, r)$. Let further $f(x)$ be an irreducible polynomial of degree $n$ over $F_2$ and $f(\alpha) = 0$.

In this case we have:

$$x^n - 1 = (x^r - 1)^{2^k} = (x+1)^{2^k}(x^{r-1} + x^{r-2} + \ldots + 1)^{2^k}.$$

Hence:

$$\Phi_1(x) = \frac{x^n - 1}{x - 1} = \sum_{j=0}^{n-1} x^j,$$

$$\Phi_2(x) = (1 + x)^{2^k} \cdot (1 + x + \dots + x^{r-1})^{2^k - 1} = (1 + x)(1 + x^r)^{2^k - 1} =$$
$$= [1 + x^r + x^{2r} + \dots + x^{(2^k - 1)\cdot r}]\cdot(1 + x).$$

Hereby we have used the fact that $\binom{2^k - 1}{v} \equiv 1 \pmod 2$ for any $v = 1, 2, \dots, 2^k - 1$. This implies:

$$\hat{\Phi}_1(\alpha) = \mathrm{Tr}(\alpha).$$
$$\hat{\Phi}_2(\alpha) = \alpha + \alpha^{2^r} + \alpha^{2^{2r}} + \dots + \alpha^{2^{n-r}} + [\alpha + \alpha^{2^r} + \dots + \alpha^{2^{n-r}}]^2 =$$
$$= S(r, \alpha) + [S(r, \alpha)]^2.$$

Now since $S(r, \alpha) \neq 0$, $\hat{\Phi}_2(\alpha) \neq 0$ if and only if $S(r, \alpha) + 1 \neq 0$.

We have the following result: The root $\alpha$ is a generator of a normal basis if and only if

a) $\mathrm{Tr}(\alpha) \neq 0$,

b) $\alpha + \alpha^{2^r} + \alpha^{2^{2r}} + \dots + \alpha^{2^{n-r}} \neq 1$.

This is the same result as given in [4].

Example 7. If $n$ is a prime-power, $n = r^e$, $e > 2$, the results obtained by our method ared formally not the same as in [4].

We first quote the main result of [4].

Proposition. Suppose $n = r^e$ ($r$ a prime, $r > 2$) and 2 is a primitive element $(\mathrm{mod}\, n)$. Let $f(x)$ be an irreducible polynomial of degree $n$ over $F_2$ and $f(\alpha) = 0$. Denote

$$g_1(x) = 1 + \sum_{u \in U_1^*} x^{2^u},$$

where

$$U_1^* = \{ir \mid i = 0, 1, 2, \dots, (r^{e-1} - 1)\} = \{0, r, 2r, \dots, (r^{e-1} - 1)r\},$$

and for $2 \leqq j \leqq e$

$$g_j(x) = \sum_{u \in U_j^*} x^{2^u}, \quad \text{where} \quad U_j^* = \{i \cdot r^{j-1} \mid i = 1, 2, \dots, (r^{e-j+1} - 1);\ r \nmid i\}.$$

Then $f(x)$ is an N-polynomial if and only if $\mathrm{Tr}(\alpha) = 1$, $g_1(\alpha) \neq 0$, $g_2(\alpha) \neq 0, \dots, g_e(\alpha) \neq 0$.

We now compare this result with the result obtained by our method in the case $e = 3$, i.e. $n = r^3$.

A) By the Proposition just mentioned $f(x)$ is an N-polynomial if and only if $\mathrm{Tr}(\alpha) = 1$ and

$$g_1(\alpha) = 1 + \sum_{u \in U_1^*} \alpha^{2^u} \neq 0, \quad \text{where} \quad U_1^* = \{ir \mid i = 0, 1, 2, \dots, r^2 - 1\},$$

$$g_2(\alpha) = \sum_{u \in U_2^*} \alpha^{2^u} \neq 0, \quad \text{where} \quad U_2^* = \{ir \mid i = 1, 2, \ldots, r^2 - 1;\ r \nmid i\},$$

$$g_3(\alpha) = \sum_{u \in U_3^*} \alpha^{2^u} \neq 0, \quad \text{where} \quad U_3^* = \{ir^2 \mid i = 1, 2, \ldots, r - 1\}.$$

B) By our method (under the same suppositions) we obtain successively: The decomposition of $x^n - 1$ into irreducible factors over $F_2$ is

$$x^n - 1 = (1 + x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot Q_{r^3}(x)$$

Hence

$$\Phi_1(x) = \sum_{i=0}^{n-1} x^i.$$

$$\Phi_2(x) = (1 + x^n)(1 + x^r)^{-1}(1 + x) = [1 + x^r + x^{2r} + \ldots + x^{(r^2-1)r}] \cdot (1 + x).$$

$$\Phi_3(x) = (1 + x^n)(1 + x^{r^2})^{-1}(1 + x^r) = [1 + x^{r^2} + x^{2r^2} + \ldots + x^{(r-1)r^2}] \cdot (1 + x^r).$$

$$\Phi_4(x) = 1 + x^{r^2}.$$

This implies:

$$\hat{\Phi}_1(\alpha) = \mathrm{Tr}\,(\alpha).$$

$$\hat{\Phi}_2(\alpha) = \sum_{u \in U_2} \alpha^{2^u}, \text{ where}$$

$$U_2 = \{0, r, 2r, \ldots, (r^2 - 1) \cdot r\} \cup \{1, r + 1, 2r + 1, \ldots, (r^2 - 1)r + 1\}.$$

$$\hat{\Phi}_3(\alpha) = \sum_{u \in U_3} \alpha^{2^u}, \text{ where}$$

$$U_3 = \{0, r^2, 2r^2, \ldots, (r - 1)r^2\} \cup \{r, r^2 + r, 2r^2 + r, \ldots, (r - 1)r^2 + r\}.$$

$$\Phi_4(\alpha) = \alpha + \alpha^{2^{r^2}}.$$

The condition $\hat{\Phi}_1(\alpha) \neq 0$ implies $\mathrm{Tr}\,(\alpha) = 1$. The condition $\hat{\Phi}_4(\alpha) \neq 0$ is always satisfied since the roots of $f(x) = 0$ are all different. The condition $\hat{\Phi}_2(\alpha) = S(r, \alpha) + S(r, \alpha)^2 \neq 0$ is satisfied (by Lemma 2) if and only if $1 + S(r, \alpha) \neq 0$. This condition is the same as the condition $g_1(\alpha) \neq 0$.

But the condition $\hat{\Phi}_3(\alpha) \neq 0$ is different from the remaining conditions $g_2(\alpha) \neq 0$ and $g_3(\alpha) \neq 0$.

To have a concrete example consider $n = 5^3$. Then

*A*) $U_2^* = \{5, 10, 15, 20, 30, 35, 40, 45, 55, 60, 65, 70, 80, 85, 90, 95, 105, 110, 115, 120\}$,

$U_3^* = \{25, 50, 75, 100\}$.

B) $U_3 = \{0, 25, 50, 75, 100\} \cup \{5, 30, 55, 80, 105\}$.

The second method leads to simpler results.

## REFERENCES

[1] CONWAY, J. H.: A tabulation of some information concerning finite fields. Computers in Mathematical Research, North-Holland, Amsterdam, 1968, 37—50.

[2] LIDL, R.—NIEDERREITER, H.: Finite Fields. Addison-Wesley Publ. Comp., Reading, Mass., 1983.

[3] ORE, O.: Contributions to the theory of finite fields. Trans. Amer. Mat. Soc. 36, 1934, 243—274.

[4] PEI, D. Y.—WANG, C. C.—OMURA, J. K.: Normal basis of finite field GF($2^m$). IEEE Trans. on Inform. Theory, IT-32, 1986, 285—287.

[5] PERLIS, S.: Normal bases of cyclic fields of prime-power degree. Duke Math. J. 9, 1942, 507—517.

[6] PETERSON, W. W.—WELDON, E. J.: Error-Correcting Codes. M.I.T. Press, Cambridge, Mass., 1972.

[7] SCHWARZ, Š.: On the reducibility of binomial congruences and the bound of the least integer belonging to a given exponent (mod p). Časop. pěst. mat. fys. 74, 1949, 1—16.

[8] SCHWARZ, Š.: On the reducibility of polynomials over a finite field. Quart. J. of Math. Oxford (2), 7, 1956, 110—124.

[9] SCHWARZ, Š.: Construction of normal bases in cyclic extensions of a field. (To appear in the Czech. Math. J.)

Received August 15, 1986

Matematický ústav SAV
Obrancov mieru 49
814 73 Bratislava

## НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД КОНЕЧНЫМ ПОЛЕМ С ЛИНЕЙНО НЕЗАВИСИМЫМИ КОРНЯМИ

Štefan Schwarz

### Резюме

Пусть $f(x)$-неприводимый многочлен степени $n$ над конечным полем $F_q$ и $f(\alpha) = 0$. Рассмотрим конечное расширение $F_q(\alpha)$ как векторное пространство размерности $n$ над $F_q$. Если корни уравнения $f(x) = 0$ линейно независимы над $F_q$ (значит они образуют нормальный базис $F_q(\alpha)/F_q$), то назовем $f(x)$ $N$-многочленом.

В статье указан общий метод проверки, является ли заданный многочлен (любой степени $n$ над любим полем $F_q$) $N$-многочленом или нет. Метод демонстрирован на нескольких примерах.