ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 111 2011 № 3

MATHEMATICS

УДК 519.4

S. Y. Abrahamyan

# Some Constructions of $N$-polynomials over Finite Fields

(Submitted by academician G. H. Khachatrian 13/V 2011)

**Key words:** *normal polynomials or $N$-polynomials, finite fields, polynomial composition*

**1. Introduction and statement of the problem.** The construction of $N$-polynomials over any finite fields is a challenging mathematical problem. Interest in $N$-polynomials stems from both mathematical theory as well as practical applications such as coding theory and cryptosystems using finite fields. The paper presents a number of results concerning the construction of $N$-polynomials over Galois fields of characteristic 2.

For a prime power $q = p^s$ and a positive integer $n$, let $F_q$ and $F_{q^n}$ be the finite fields with $q$ and $q^n$ elements, respectively.

A *normal* basis $N$ for $F_{q^n}$ over $F_q$ is a basis of the form $N = N_\alpha := \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ for some element $\alpha \in F_{q^n}$, i.e., a basis that consists of the orbit of an element $\alpha \in F_{q^n}$ relative to the Galois group of $F_{q^n}$ over $F_q$. Any element $\alpha \in F_{q^n}$ for which that orbit is such a basis is said to be a *normal element* in, or *normal basis generator* for, $F_{q^n}$ (over $F_q$).

A monic irreducible polynomial $F(x) \in F_q[x]$ is called *normal* if its roots form a normal basis or, equivalently, if they are linearly independent over $F_q$. Following Schwarz [1], we shall call these polynomials *$N$-polynomials*.

The *minimal* polynomial of an element in a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is $m(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i}) \in F_q[x]$, which is irreducible over $F_q$. The elements in a normal basis are exactly the roots of some $N$-polynomial.

The problem in general is: given an integer $n$ and the ground field $F_q$, construct a normal basis of $F_{q^n}$ over $F_q$ or, equivalently, construct an $N$-polynomial in $F_q[x]$ of degree $n$.

Some results regarding computationally simple constructions of $N$-polynomials over $F_q$ can be found in [2]-[6]. Iterative constructions of irreducible polynomials of 2-power degree over finite fields of odd characteristics are given in Cohen [7] and McNay [8]. Meyn [5] and Chapman [2] have shown that these polynomials are $N$-polynomials. In particular, one may start with any irreducible polynomial $f_0(x) \in F_2$ of degree $n$ for which the coefficients of $x^{n-1}$ and $x$ are both 1. Kyuregyan in [9] has derived a number of generalizations and in [10, 11] considered constructions which yield sequences of normal irreducible polynomials.

**2. Preliminaries.** We'll begin with recalling some definitions and basic results on the irreducibility and normality of polynomials that will be helpful to derive our main result.

**Theorem 1 (Cohen [7].)** *Let $f(x), g(x) \in F_q[x]$ be relatively prime polynomials and let $P(x) \in F_q[x]$ be an irreducible polynomial of degree $n$. Then the composition*

$$F(x) = g^n(x)P\big(f(x)/g(x)\big)$$

*is irreducible over $F_q$ if and only if $f(x) - \alpha g(x)$ is irreducible over $F_{q^n}$ for some root $\alpha \in F_{q^n}$ of $P(x)$.*

**Proposition 1 ([12], Theorem 3.78.)** *Let $\alpha \in F_q$ and let $p$ be the characteristic of $F_q$. Then the trinomial $x^p - x - \alpha$ is irreducible in $F_q[x]$ if and only if it has no root in $F_q$.*

**Proposition 2 ([12], Corollary 3.79.)** *With the notation of Proposition 1 the trinomial $x^p - x - \alpha$ is irreducible in $F_q[x]$ if and only if $Tr_{F_q}(\alpha) \neq 0$.*

The trace function of $F_{q^n}$ over $F_q$ is defined as:

$$Tr_{q^n/q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i},\ \alpha \in F_{q^n}$$

The trace function is a linear functional from $F_{q^n}$ to $F_q$. For convince denote the trace function as $Tr_{q^n/q}$. The trace of an element over its characteristic subfield is called *absolute trace.* Recall that the Frobenius map:

$$\sigma : \eta \rightarrow \eta^q,\ \eta \in F_{q^n}$$

is an automorphism of $F_{q^n}$ that fixes $F_q$.

In particular, $\sigma$ is a linear transformation of $F_{q^n}$ viewed as a vector space of dimension $n$ over $F_q$. By definition, $\alpha \in F_{q^n}$ is a normal element over $F_q$ if and only if $\alpha, \sigma\alpha = \alpha^q, \sigma^2\alpha = \alpha^{q^2}, \ldots, \sigma^{n-1}\alpha = \alpha^{q^{n-1}}$ are linearly independent over $F_q$.

To characterize all the normal elements, we determine the minimal and characteristic polynomials of $\sigma$.

**Proposition 3** . *The minimal and characteristic polynomial for $\sigma$ are identical, both being $x^n - 1$.*

For any polynomial $g(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathrm{F}_q[x]$, define $g(\sigma)\eta = \left(\sum_{i=0}^{n-1} g_i \sigma^i\right)\eta = \sum_{i=0}^{n-1} g_i \eta^{q^i}$ which is also a linear transformation on $\mathrm{F}_{q^n}$.

For any element $\alpha \in \mathrm{F}_{q^n}$, the monic polynomial $g(x) \in \mathrm{F}_q[x]$ of the smallest degree such that $g(\sigma)\alpha = 0$ is called the $\sigma$-order of $\alpha$ (some authors call it the $\sigma$-annihilator, the minimal polynomial, or the additive order of $\alpha$). We denote this polynomial by $\mathrm{Ord}_{\alpha,\sigma}(x)$. Note that $\mathrm{Ord}_{\alpha,\sigma}(x)$ divides any polynomial $h(x)$ annihilating $\alpha$ (i.e. $h(\sigma)\alpha = 0$). In particular, for every $\alpha \in \mathrm{F}_{q^n}$, $\mathrm{Ord}_{\alpha,\sigma}(x)$ divides $x^n - 1$, the minimal or characteristic polynomial for $\sigma$.

Our objective is to locate the normal elements in $\mathrm{F}_{q^n}$ over $\mathrm{F}_q$. Let $\alpha \in \mathrm{F}_{q^n}$ be a normal element. Then $\alpha,\ \sigma\alpha\ \dots,\ \sigma^{n-1}\alpha$ are linearly independent over $\mathrm{F}_q$. So there is no polynomial of degree less than $n$ that annihilates $\alpha$ with respect to $\sigma$. Hence, according to Proposition 3, the $\sigma$-order of $\alpha$ must be $x^n - 1$, that is $\alpha$ is a cyclic vector of $\mathrm{F}_{q^n}$ over $\mathrm{F}_q$ with respect to $\sigma$. So an element $\alpha \in \mathrm{F}_{q^n}$ is a normal element over $\mathrm{F}_q$ if and only if $\mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$.

Let $n = n_0 2^e$ with $\gcd(2, n_0) = 1$ and $e \geq 0$. For convenience, we denote $2^e$ by $t$. Suppose that $x^n + 1 = (x^{n_0} + 1)^t$ has the following factorization in $\mathrm{F}_{2^s}[x]$:

$$x^n + 1 = \big(\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x)\big)^t \tag{1}$$

where $\varphi_i(x) \in \mathrm{F}_{2^s}[x]$ are the distinct irreducible factors of $x^{n_0} + 1$.

Let

$$\Phi_i(x) := \frac{x^n - 1}{\varphi_i(x)} = \sum_{\mu=0}^{m_i} t_{i\mu}\, x^{\mu},\ i = 1, 2, \dots, r \tag{2}$$

Further, let $L_{\Phi_i}(x)$ denote the corresponding *linearized* polynomial defined by

$$L_{\Phi_i}(x) := \sum_{\mu=0}^{m_i} t_{i\mu}\, x^{q^{\mu}}.$$

We will need Schwartz's theorem (Theorem 4.18 of Chapter 4 in [4]) which allows us to check whether an irreducible polynomial is an $N$-polynomial.

**Proposition 4 (Theorem 4.18, [4].)** *Let $F(x)$ be a monic irreducible polynomial of degree n over $\mathrm{F}_q$, and let $\alpha$ be and a root of the polynomial. Then, $F(x)$ is an $N$-polynomial over $\mathrm{F}_q$ if and only if*

$$L_{\Phi_i}(\alpha) \neq 0 \quad \textit{holds for each} \quad i = 1, 2, \dots, r.$$

Next we present a result by Jungnickel [13] that states when an element of $F_q$ is a normal bases generator.

**Proposition 5 [13].** *Let $\alpha$ be a generator for a normal basis $N$ of $F_{q^n}$ over $F_q$ and let $a, b \in F_q^*$. Then $\gamma = a + b\alpha$ is also a normal basis generator if and only if one has*

$$na + bTr(\alpha) \neq 0.$$

With these preliminaries we state a theorem that yields an $N$- polynomial of degree $n$ over $F_{2^s}$.

**3. Construction of $N$-Polynomials.** In this section we shall establish the normality of the composite polynomial $F(x) = (x^2 + x + 1)^n P\left(\frac{x^2+x}{x^2+x+1}\right)$ over $F_{2^s}$.

**Theorem 2** . *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree $n \geq 2$ over $F_{2^s}$, $P^*(x)$ be a normal polynomial and let*

$$F(x) = \left(x^2 + x + 1\right)^n P\left(\frac{x^2 + x}{x^2 + x + 1}\right). \tag{3}$$

*Then $F^*(x)$ is an $N$-polynomial of degree $2n$ over $F_{2^s}$ if*

$$Tr_{2^s/2}\left(\frac{P'(1)}{P(1)} + n\right) \neq 0 \text{ and } \frac{c_1}{c_0} + n \neq 0.$$

**Proof.** First we shall show that $F(x)$ is an irreducible polynomial. By Theorem 1 the polynomial $F(x)$ is irreducible over $F_{2^s}$ if and only if $(1+\alpha)\,x^2 - (1+\alpha)\,x + \alpha$ is irreducible over $F_{2^{sn}}$, where $\alpha \in F_{2^{sn}}$ is a root of $P(x)$. And by proposition 1 $(1+\alpha)\left(x^2 + x + \frac{\alpha}{(\alpha+1)}\right)$ is irreducible over $F_{2^{sn}}$ if and only if $Tr_{2^{sn}/2}\left(\frac{\alpha}{\alpha+1}\right) \neq 0$.

From the properties of trace we will have

$$Tr_{2^{sn}/2}\left(\frac{\alpha}{\alpha+1}\right) = Tr_{2^s|2}\left(Tr_{2^{sn}/2^s}\ \frac{1}{\alpha+1} + n\right).$$

Next we compute the trace

$$Tr_{2^{sn}/2^s}\left(\frac{1}{\alpha+1}\right).$$

We denote $P\,(x+1)$ as follows:

$$P\,(x+1) = \sum_{i=0}^{n} c_i\,(x+1)^i = \sum_{i=0}^{n} d_i x^i = D(x).$$

Since $\alpha$ is a root of $P(x)$ then $\alpha+1$ must be a root of $D(x) = P\,(x+1)$ and therefore $\frac{1}{\alpha+1}$ is a root of $D^*(x)$ (recall here that $D^*(x)$ is a reciprocal polynomial of $D(x)$). Then

$$Tr_{2^{sn}/2^s}\left(\frac{1}{\alpha+1}\right) = \frac{d_1}{d_0}.$$

Next we compute $d_1$ and $d_0$

$$\begin{aligned} d_0 &= D(0) = \sum_{i=0}^{n} c_i = P(1) \\ d_1 &= D'(0)^1 = P'(x+1)\Big|_{x=0} = \sum_{i=0}^{n} i\ c_i = P'(1)\,. \end{aligned}$$

$$Tr_{2^{sn}/2^s}\left(\frac{1}{\alpha+1}\right) = \frac{d_1}{d_0} = \frac{P'(1)}{P(1)}$$

and

$$Tr_{2^s/2}\left(\frac{\alpha}{\alpha+1}\right) = Tr_{2^s/2}\left(\frac{P'(1)}{P(1)} + n\right).$$

We proceed by proving that $F^*(x)$ is a normal polynomial. Let $\alpha_1$ be a root of $F(x)$. Then, evidently $\beta_1 = \frac{1}{\alpha_1}$ is a root of its reciprocal polynomial $F^*(x)$. We only need to show that $\sigma$-order of $\beta_1$ is

$$Ord_{\beta_1,\sigma}(x) = x^{2n} + 1$$

Note that by (1) the polynomial $x^{2n}+1$ has the following factorization in $F_{2^s}[x]$:

$$x^{2n} + 1 = (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^{2t}$$

where $\varphi_i(x) \in F_{2^s}[x]$ are distinct irreducible factors of $x^{2n}+1$. Let

$$H_i(x) = \frac{x^{2n}+1}{\varphi_i(x)} = \frac{(x^n+1)(x^n+1)}{\varphi_i(x)}.$$

By (2) we have

$$H_i(x) = \sum_{v=0}^{m_i} t_{iv}\left(x^{n+v} + x^v\right).$$

Then it follows that

$$\begin{aligned} L_{H_i}(\beta_1) &= \sum_{v=0}^{m_i} t_{iv}\left((\beta_1)^{(2^s)^{n+v}} + (\beta_1)^{(2^s)^v}\right) \\ &= \sum_{v=0}^{m_i} t_{iv}\left(\left(\frac{1}{\alpha_1}\right)^{2^{sn}} + \left(\frac{1}{\alpha_1}\right)\right)^{2^{sv}} = \sum_{v=0}^{m_i} t_{iv}\left(\frac{1+\alpha_1^{2^{sn}-1}}{\alpha_1^{2^{sn}+1}}\right)^{2^{sv}}. \end{aligned}$$

By (3) we may assume that

$$\alpha + 1 = \left(\alpha_1^2 + \alpha_1 + 1\right)^{-1}. \tag{4}$$

As $\alpha \in F_{2^{sn}}$ we have

$$\alpha + 1 = (\alpha+1)^{2^{sn}} = \left(\alpha_1^{2^{sn+1}} + \alpha_1^{2^{sn}} + 1\right)^{-1}. \tag{5}$$

[1] $D'(x)$ is a formal derivative of $D(x)$.

From (4) and (5) it follows that

$$\left(\alpha_1^2+\alpha_1+1\right)^{-1}=\left(\alpha_1^{2^{sn+1}}+\alpha_1^{2^{sn}}+1\right)^{-1}.$$

Since $\alpha_1^2+\alpha_1+1\neq 0$ we may imply that

$$\left(\alpha_1^{2^{sn}}+\alpha_1\right)\left(\alpha_1^{2^{sn}}+\alpha_1+1\right)=0 \text{ and } (\alpha+1)^{-1}=\alpha_1^2+\alpha_1+1. \tag{6}$$

As $\alpha_1^{2^{sn}}+\alpha_1\neq 0$ we shall have

$$\left(\alpha_1^{2^{sn}-1}+1\right)=\frac{1}{\alpha_1}. \tag{7}$$

From (7) we obtain

$$H_i(\beta)=\sum_{v=0}^{m_i} t_{iv}\left(\frac{1}{\alpha_1^2+\alpha_1}\right)^{2^{sv}}.$$

From (6) one can imply that

$$\alpha_1^2+\alpha_1=\frac{1}{\alpha+1}+1=\frac{\alpha}{\alpha+1}. \tag{8}$$

Substitution of (8) in (7) gives

$$H_i(\beta)=\left(\sum_{v=0}^{m_i} t_{iv}\,\frac{\alpha+1}{\alpha}\right)^{2^{sv}}=\left(\sum_{v=0}^{m_i} t_{iv}\left(\frac{1}{\alpha}+1\right)\right)^{2^{sv}}.$$

Denote $P^*(x)$ by $k(x)$. As $k(x)$ is a normal polynomial, then according to Proposition 5 $k(x+1)$ will also be normal if and only if

$$Tr_{2^{sn}/2^s}\left(\frac{1}{\alpha}\right)+n\neq 0 \text{ or } \frac{c_1}{c_0}+n\neq 0.$$

And because $\frac{1}{\alpha}+1$ is a root of the normal polynomial $k(x+1)$, hence

$$\sum_{v=0}^{m_i} t_{iv}\,\left(\frac{1}{\alpha}+1\right)\neq 0.$$

The proof of the theorem is completed.

**Acknowledgment.** This study was supported by the grant ('GRASP-10-05') of the National Academy of Sciences of RA, the National Foundation of Science and Advanced Technologies (RA) and Civilian Research and Development Foundation (US).

Institute for Informatics and Automation Problems of NAS RA

**S. Y. Abrahamyan**

**Some Constructions of $N$-polynomials over Finite Fields**

The problem of constructing irreducible polynomials over $\mathbb{F}_{2^s}$ with linearly independent roots or normal polynomials or $N$-polynomials over the field $\mathbb{F}_{2^s}$ is considoxed. For a suitably chosen initial $N$-polynomial $F_0(x) \in \mathbb{F}_{2^s}[x]$ of degree $n$, an $N$-polynomial $F(x) \in \mathbb{F}_{2^s}[x]$ of degree $2n$ is constructed by using the polynomial composition method.

**Ս. Ե. Աբրահամյան**

**Վերջավոր դաշտերի վրա նորմալ բազմանդամների կառուցումն**

Դիտարկված է $\mathbb{F}_{2^s}$ դաշտի վրա գծորեն-անկախ արմատներով չբերվող բազմանդամների այսպես կոչված նորմալ կամ $N$-բազմանդամների կառուցման խնդիրը: Համապատասխանաբար ընտրված սկզբնական $n$ աստիճանի $N$-բազմանդամից $\mathbb{F}_{2^s}[x]$ օղակում կառուցվել է $2n$ աստիճանի $N$-բազմանդամ $\mathbb{F}_{2^s}[x]$-ում՝ բազմանդամների կոմպոզիցիոն մեթոդի օգնությամբ:

**С. Е. Абрамян**

**Построение нормальных полиномов над конечными полями**

Рассмотрена проблема построения многочленов с линейно независимыми корнями или нормальных многочленов или $N$-многочленов над полем $\mathbb{F}_{2^s}$. Исходя из начального $N$-многочлена степени $n$ в $\mathbb{F}_{2^s}[x]$ построен многочлен степени $2n$ в $\mathbb{F}_{2^s}[x]$ посредством метода полиномиальной композиции.

# References

[1] *Schwartz S.* -Math. Slovaca. 1988. V. 38. P.147-158.

[2] *Chapman R.* - J. Finite Fields and Their Applications, 1997. V.3 P. 3-10.

[3] *Gao S.* - Normal bases over finite fields. Ph.D. Thesis, Waterloo, 1993.

[4] *Menezes A.J., Blake I.F., Gao X., Mullin R.C., Vanstone S.A. and Yaghoobian T.*. Applications of finite fields. Kluwer Academic Publishers, Boston-Dordrecht-Lancaster. 1993.

[5] *Meyn H.* - Designs, Codes and Cryptography. 1995. V.6. P.107-116.

[6] *Varshamov R. R.* - Soviet Math. Dokl. 1984. V.29. P.334 − 336.

[7] *Cohen S. D.* - Designs, Codes and Cryptography, 1992. V.2. P. 169-174.

[8] *McNay G.*. Topics in finite fields. Ph.D. thesis, University of Glasgow, 1995.

[9] *Kyuregyan M. K.* - Finite Fields and Their Applications. 2002. V. 8. P. 52-68.

[10] *Kyuregyan M. K.*- Finite Fields and Their Applications. 2004. V.10. P. 323-431.

[11] *Kyuregyan M.K.* Discrete Applied Mathematics. 2008. V. 156. 1554 − 1559.

[12] *Lidl R. and Niederreiter H.* Finite Fields. Cambridge University Press. 1987.

[13] *Jungnickel D.* - Dicrete Applied Mathematics. 1993. V.47. P. 233-249.