ЦЗЦИВЦЬ ФРОПОВЛЬТЬ С ЦАЦАВИТНАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИNATIONAL ACADEMY OF SCIENCES OF ARMENIAДОКЛАДЫ254ЛЬЗЗТЬРREPORTS

111 11	2011	No 3

MATHEMALICS

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 composilion

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 $q = p^{*}$ and a positive integer n, let \mathbb{F}_{q} and $\mathbb{F}_{q^{n}}$ be the finite helds with q and q^{n} elements, respectively.

A normal basis N for \mathbb{F}_{q^n} over \mathbb{F}_q is a basis of the form $N = N_{\alpha} = \dots \alpha^{q^n}$ } for some element $\alpha \in \mathbb{F}_{q^n}$, i.e., a basis that consists of the orbit of an element $\alpha \in \mathbb{F}_{q^n}$ relative to the Galois group of \mathbb{F}_{q^n} over \mathbb{F}_q . Any element $\alpha \in \mathbb{F}_{q^n}$ for which that orbit is such a basis is said to be a normal element in, or normal basis generator for, \mathbb{F}_{q^n} (over \mathbb{F}_q).

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

The minimal polynomial of an element in a normal basis $\{\alpha, \alpha^q, ..., \}$ is $m(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}) \in [n]$, which is irreducible over \mathbb{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 \mathbb{F}_q , construct a normal basis of \mathbb{F}_{q^n} over \mathbb{F}_q or, equivalently, construct an N-polynomial in $\mathbb{F}_q[r]$ of degree n.



regarding computationally simple constructions of Nresults Some polynomials over \mathbb{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 $f_0(x) \in \mathbb{F}_2$ of degree n for which the coefficients of x^{n-1} and x are both I. 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 $f(x), g(x) \in \mathbb{F}_q[x]$ be relatively prime polynomials and let $| (\in \mathbb{F}_{q} | x | bc an irreducible polynomial of degree n. Then the composition$

 $F(x) = g^{n}(x)P(f(x)/g(x))$

invaluable over \mathbb{F}_q , if and only if $f(x) - \alpha g(x)$ is irreducible over \mathbb{F}_{q^n} for some real $\alpha \in \mathbb{F}_{q^n}$ of P(x).

Proposition 1 ([12], Theorem 3.78). Let $\alpha \in \mathbb{F}_q$ and let p be the characteristic of \mathbb{F}_q . Then the transmal $x^p - x - \alpha$ is irreducible in $\mathbb{F}_q[x]$ if and only if it has no root in \mathbb{F}_q .

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

The trace function of \mathbf{F}_q over \mathbf{F}_q is defined as:

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

The trace function is a linear functional from \mathbb{F}_{q^2} to \mathbb{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:

$$\sigma:\eta\to\eta^q,\,\eta\in\mathbb{F}_{q^n}$$

is an automorphism of \mathbb{F}_{q^n} that fixes \mathbb{F}_{q^n}

In particular, σ is a linear transformation of Γ , viewed as a vector space of dimension n over \mathbb{F}_q . By definition, $\alpha \in \mathbb{F}_{q^n}$ is a normal element over \mathbb{F}_q if and only if $\alpha, \sigma \alpha = \alpha^{q}, \sigma^{2} \alpha = \alpha^{q^{2}}, \dots, \sigma^{n-1} \alpha = \alpha^{q^{n-1}}$ are linearly independent over \mathbb{F}_{q} .

To characterize all the normal elements, we determine the minimal and characteristic polynomials of σ .



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

For any polynomial
$$g(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{F}_q[x]$$
, define $g(\sigma)\eta = \left(\sum_{i=0}^{n-1} g_i \sigma^i\right)\eta =$

 $\sum_{q,\eta} g_{\eta} \eta^{q}$ which is also a linear transformation on \mathbb{F}_{q^n} .

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

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

over \mathbb{F}_q if and only if $\operatorname{Ord}_{\alpha,\sigma}(x) = x^n - 1$.

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

$$x^{n} + 1 = \left(\varphi_{1}(x)\varphi_{2}(x)\cdots\varphi_{r}(x)\right)^{r} \tag{1}$$

where $\varphi_{\cdot}(x) \in \mathbb{F}_{2^{*}}[x]$ are the distinct irreducible factors of $x^{n_{0}} + 1$. Let

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

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

$$L_{\Phi_i}(x) := \sum_{\mu=0}^{m_1} t_{i\mu} \ x^{q^{\mu}}.$$

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 F_{ij} and let α be and a root of the polynomial. Then, F(x) is an N-polynomial over F_{ij} if and only if

$$1 \quad (1) \neq 0$$
 holds for each $i = 1, 2, \ldots, r$.



Next we present a result by Jungnickel [13] that states when an element of \mathbb{F}_n is a normal bases generator.

Proposition 5 [13]. Let α be a generator for a normal basis of \mathbf{F}_{q^n} over \mathbf{F}_q and let $a, b \in \mathbb{F}$. 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 \mathbb{F}_{2^s} .

3. Construction of N-Polynomials. In this section we shall establish the normality of the composite polynomial $F(x) = (x^2 + x + 1)^n P(\frac{x^2 + x}{x^2 + x - 1})$ over \mathbb{F}_2 .

Theorem 2 Let $P(x) = \sum_{i=1}^{n} c_i x^i$ be an irreducible polynomial of degree $n \ge 2$ over \mathbb{F}_{2^*} . $P^*(x)$ be a normal polynomial and let

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

Then $F^{\bullet}(x)$ is an N-polynomial of degree 2n over $\mathbb{F}_{2^{\bullet}}$ if

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

Proof. First we shall show that F(x) is an irreducible polynomial. By Theorem 1 the polynomial F(x) is irreducible over \mathbb{F}_{2^n} if and only if $(1 + \alpha) x^n - (1 + \alpha) x^n - (1$

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

Next we compute the trace

$$l' \tau_{2^{sn}/2^s} \left(\frac{1}{\alpha+1} \right)$$

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

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



Next we compute d_1 and d_0

$$d_0 = D(0) = \sum_{i=0}^{n} c_i = P(1)$$

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

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

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 α_{1} be a root of F(x). Then, evidently $\beta_1 = -$ is a root of its reciprocal polynomial $F^*(x)$. We only need to show that σ -order of β_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_{n-1}

$$x^{-m} + 1 = (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^{-1}$$

where $\rho_1(x) \in F_{2^*}[x]$ 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

$$H_{\iota}(x)=\sum_{\nu=0}^{m_{\iota}}t_{\iota\nu}\left(x^{n+\nu}+x^{\nu}\right).$$

Then it follows that

$$L_{II_{i}}(\beta_{1}) = \sum_{v=0}^{m_{i}} t_{iv} \left((\beta_{1})^{(2^{*})^{n+v}} + (\beta_{1})^{(2^{*})^{v}} \right)$$

$$= \sum_{v=0}^{m_{i}} t_{iv} \left(\left(\frac{1}{\alpha_{1}} \right)^{2^{sn}} + \left(\frac{1}{\alpha_{1}} \right) \right)^{2^{sv}} = \sum_{v=0}^{m_{i}} t_{iv} \left(\frac{1 + \alpha_{1}^{2^{sn} - 1}}{\alpha_{1}^{2^{sn} + 1}} \right)^{2^{sv}}$$

By (3) we may assume that

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

As $\alpha \in \mathbb{F}_{2^{n}}$ we have

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



D'(r) is a formal derivative of D(r)

From (4) and (5) it follows that

$$(\alpha_1^2 + \alpha_1 + 1)^{-1} = (\alpha_1^{2^{n+1}} + \alpha_1^{2^{n}} + 1)^{-1}$$

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

$$(\alpha_1^{2^{*n}} + \alpha_1)(\alpha_1^{2^{*n}} + \alpha_1 + 1) = 0$$
 and $(\alpha + 1)^{-1} = \alpha_1^2 + \alpha_1 + 1.$ (6)

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

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

From (7) we obtain

$$H_{i}\left(\beta\right) = \sum_{\nu=0}^{m_{i}} t_{i\nu} \left(\frac{1}{\alpha_{1}^{2} + \alpha_{1}}\right)^{2^{*\nu}}.$$

From (6) one can imply that

$$\alpha_1^2 + \alpha_1 = \frac{1}{\alpha + 1} + 1 = \frac{\alpha}{\alpha + 1}$$
(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

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

And because - + 1 is a root of the normal polynomial k(x + 1), hence

$$\sum_{\nu=0}^{m_{i}} t_{i\nu} \left(\frac{1}{\alpha}+1\right) \neq 0.$$

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

Ս. Ե. Արրահամյան

Վերջավոր դաշտերի վրա նորմալ բազմանդամների կառուցում

Դիտարկված է \mathbb{F}_{2^*} դաշտի վրա գծորեն-անկախ արմափներով չբերվող բազմանդամների այսպես կոչված նորմալ կամ N-բազմանդամների կառուցման խնդիրը <ամապատասխանա բար ընտրված սկզբնական π աստիճանի N բազմանդամից $\mathbb{F}_{2^*}[x]$ օղակում կառուզվել է 2nաստիճանի N-բազմանդամ $\mathbb{F}_{2^*}[x]$ -ում՝ բազմանդամների կոսպոզիցիոն 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 **F**₂. Исходя из начального *N*-многочлена степени *n* в **[***x***]** построен многочлен степени 2*n* в **[***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] M. Nay G Topics in finite fields Ph.D, thesis, University of Glasgow 1995
- [9] Kyuregyun 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] Kyuregyun 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

