International Journal of Algebra, Vol. 5, 2011, no. 29, 1437 - 1442

Constructing N-Polynomials over Finite Fields

Mahmood Alizadeh

Islamic Azad University- Ahvaz Branch
Ahvaz, Iran
Alizadeh@iauahvaz.ac.ir

Sergey Abrahamyan

Institute for Informatics and Automation Problems
Yerevan, Armenia
serj.abrahamyan@gmail.com

Saeid Mehrabi

Esfahan Payame Noor University
Esfahan, Iran
saeid_mehrabi@yahoo.com

Melsik K. Kuyregyan

Institute for Informatics and Automation Problems
National Academy of Sciences of Armenia
Yerevan, Armenia
melsik@ipia.sci.am

Abstract

This paper is devoted to the composition of constructing families of Normal polynomials over the finite field of Characteristic three.

Mathematics Subject Classification: 12A20

Keywords: Galois fields, N-polynomials, Irreducible polynomials

1 Introduction

The problem of normality of polynomials over Galois fields is a case of spacial interest and plays an important role in modern engineering.

Let F_q, be a Galois field of order $q = p^s$, where p is a prime and s is a natural number and F_q^*, be its multiplicative group. A normal basis N for F_{q^n} over F_q is a basis of the form $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ for some element $\alpha \in F_{q^n}$.

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. This paper presents a result on the theory of the synthesis of Normal polynomials (N-Polynomials) over F_{3^s}.

Some results regarding computationally simple costructions of N-polynomials over F_q can be found in [3, 6, 7]. Also kyuregyan in [4, 5] cosidered constructions which yield sequences of normal irreducible polynomials.

2 Preliminary Notes

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.

Definition 2.1 *Let F_{q^n} be a finite extension field of the finite field F_q. For $\alpha \in F_{q^n}$, the trace $Tr_{q^n|q}(\alpha)$ over F_q is defined by*

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}.$$

Let $n = n_1 p^e = n_1 t$, with $gcd(p, n_1) = 1$ and suppose that $x^n - 1$ has the following factorization in F_q

$$x^n - 1 = (x^{n_1} - 1)^t = (\varphi_1(x)\varphi_2(x)...\varphi_r(x))^t. \tag{1}$$

Set

$$\phi_i(x) = \frac{x^n - 1}{\varphi_i(x)} = \sum_{v=0}^{m_i} t_{iv} x^v$$

We will need the following theorem which allows us to check if an irreducible polynomial is an N-polynomial.

Proposition 2.1(Theorem 4.8, [6]). Let $F(x)$ be an irreducible polynomial of degree n over F_q and α be a root of it. Let $x^n - 1$ factors as above and let $\phi_i(x)$ be as in above. Then $F(x)$ is an N-polynomial over F_q if and only if

$$L_{\phi_i}(\alpha) \neq 0 \ for \ i = 1, 2, ..., r$$

where $L_{\phi_i}(x)$ is the linearized polynomial defined by $L_{\phi_i}(x) = \sum_{v=0}^{m_i} t_{iv} x^{q^v}$ if $\phi_i(x) = \sum_{v=0}^{m_i} t_{iv} x^v$.

Proposition 2.2 ([1], Theorem 1). Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be irreducible over F_q of degree n and let $\delta_0, \delta_1 \in F_q$, $\delta_0 \neq \delta_1$. then

$$F(x) = (x^p - x + \delta_1)^n P(\frac{x^p - x + \delta_0}{x^p - x + \delta_1})$$

is irreducible polynomial of degree pn over F_q if and only if

$$Tr_{q|p}((\delta_1 - \delta_0)\frac{P'(1)}{P(1)} - n\delta_1) \neq 0$$

Lemma 2.2 *(D. Jungnickel, [2]) Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a N-polynomial of degree n over $F_q (q = p^s)$. Then the polynomial $g(x) = f(\frac{x-a}{b})$ is a N-polynomial if and only if $na - bc_{n-1} \neq 0$.*

Proof. Let $n = n_1 p^e = n_1 t$, then by (1), $x^n - 1$ has the following factorization in F_q

$$x^n - 1 = (x^{n_1} - 1)^t = (\varphi_1(x)\varphi_2(x)...\varphi_r(x))^t,$$

where put $\varphi_1(x) = x - 1$. Set for $i = 2, 3, ..., r$

$$\phi_i(x) = \frac{x^n - 1}{\varphi_i(x)} = (x-1)^t s_i(x) = (x-1)s_i'(x),$$

where

$$s_i'(x) = (x-1)^{t-1} s_i(x) = \sum_{v=0}^{m_i} t_{iv} x^v.$$

Hence

$$\phi_i(x) = \sum_{v=0}^{m_i} t_{iv} x^{v+1} - \sum_{v=0}^{m_i} t_{iv} x^v.$$

Because $f(x)$ is N-polynomial, we have $L_{\phi_i}(\alpha) \neq 0$ for $i = 1, 2, ..., r$, where α is a root of $f(x)$. We show that we can derive also $L_{\phi_i}(a + b\alpha) \neq 0$, for $i = 2, 3, ..., r$, where $a + b\alpha$ is a root of $g(x)$. Since

$$\begin{aligned} L_{\phi_i}(a + b\alpha) &= \sum_{v=0}^{m_i} t_{iv}(a + b\alpha)^{q^{v+1}} - \sum_{v=0}^{m_i} t_{iv}(a + b\alpha)^{q^v} \\ &= a\sum_{v=0}^{m_i} t_{iv} + b\sum_{v=0}^{m_i} t_{iv}\alpha^{q^{v+1}} - a\sum_{v=0}^{m_i} t_{iv} - b\sum_{v=0}^{m_i} t_{iv}\alpha^{q^v} \\ &= b(\sum_{v=0}^{m_i} t_{iv}\alpha^{q^{v+1}} - \sum_{v=0}^{m_i} t_{iv}\alpha^{q^v}) = bL_{\phi_i}(\alpha) \neq 0 \end{aligned}$$

So for being $g(x)$, N-polynomial we need to find a condition that $L_{\phi_1}(a+b\alpha) \neq 0$. But we have

$$\phi_1(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + ... + x + 1 = \sum_{i=0}^{n-1} x^i.$$

So

$$\begin{aligned} L_{\phi_1}(a + b\alpha) &= \sum_{i=0}^{n-1}(a + b\alpha)^{q^i} = \sum_{i=0}^{n-1} a + b\sum_{i=0}^{n-1} \alpha^{q^i} \\ &= na + bTr_{q^n|q}(\alpha) = na - bc_{n-1}. \end{aligned}$$

This completes the proof.

3 constructing N-polynomials over finite fields

The following theorem shows if $P(x)$ be a N-polynomial of degree n over F_{3^s}, how proposition 2.2 can be used to produce a new N-polynomial of degree $3n$ over F_{3^s}.

Theorem 3.1 *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over F_{3^s} and $P^*(x)$ be a N-polynomial over F_{3^s}. Also let*

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

Then $F^*(x)$ is a N-polynomial of degree $3n$ over F_{3^s} if and only if

$$(n + \frac{c_1}{c_0}) \cdot Tr_{q|p}(\frac{P'(1)}{P(1)} - n) \neq 0$$

Proof. proposition 2.2 and theorem's hypothesis implies that $F(x)$ is irreducible over F_{3^s}. On the other side by (1) We have

$$x^{3n} - 1 = (\varphi_1(x) \cdot \varphi_2(x) \cdot ... \cdot \varphi_r(x))^{3t}.$$

where $\varphi_i(x) \in F_{3^s}[x]$ are distinct irreducible factors of $x^n - 1$. Let

$$\begin{aligned} H_i(x) = \frac{x^{3n} - 1}{\varphi_i(x)} &= \frac{(x^n - 1)(x^{2n} + x^n + 1)}{\varphi_i(x)} \\ &= \sum_{v=0}^{m_i} t_{iv} x^v (x^{2n} + x^n + 1)) \\ &= \sum_{v=0}^{m_i} t_{iv}(x^{2n+v} + x^{n+v} + x^v)) \end{aligned} \tag{3}$$

where

$$\frac{(x^n-1)}{\varphi_i(x)} = \sum_{v=0}^{m_i} t_{iv}x^v.$$

Suppose that α_1 be a root of $F(x)$. Then $\beta_1 = \frac{1}{\alpha_1}$ is a root of $F^*(x)$.We must show that

$$L_{H_i}(\beta_1) \neq 0$$

But

$$L_{H_i}(\beta_1) = \sum_{v=0}^{m_i} t_{iv}(\beta_1^{(3^s)^{2n+v}} + \beta_1^{(3^s)^{n+v}} + \beta_1^{(3^s)^v})$$

$$= \sum_{v=0}^{m_i} t_{iv}((\frac{1}{\alpha_1})^{3^{2sn}} + (\frac{1}{\alpha_1})^{3^{sn}} + (\frac{1}{\alpha_1}))^{3^{sv}}. \tag{4}$$

We note that by (2), $\frac{{\alpha_1}^3-\alpha_1}{{\alpha_1}^3-\alpha_1+1}$ is a root of $P(x)$. So we may assume that

$$\alpha = \frac{{\alpha_1}^3-\alpha_1}{{\alpha_1}^3-\alpha_1+1},$$

where α is a root of $P(x)$. Hence we have

$$\alpha - 1 = \frac{{\alpha_1}^3-\alpha_1}{{\alpha_1}^3-\alpha_1+1} - 1 = \frac{-1}{{\alpha_1}^3-\alpha_1+1}$$

or equivalently

$$\alpha - 1 = -({\alpha_1}^3-\alpha_1+1)^{-1} \tag{5}$$

so by (5) we have

$${\alpha_1}^3-\alpha_1 = \frac{\alpha}{1-\alpha} \tag{6}$$

also by (5)

$$(\alpha-1)^{3^{sn}} = \alpha - 1 = -({\alpha_1}^{3^{sn+1}} - {\alpha_1}^{3^{sn}} + 1)^{-1}. \tag{7}$$

Then (7) and (5) implies that

$$({\alpha_1}^{3^{sn+1}} - {\alpha_1}^{3^{sn}} + 1)^{-1} = ({\alpha_1}^3 - \alpha_1 + 1)^{-1}.$$

But $({\alpha_1}^3 - \alpha_1 + 1) \neq 0$, so we have

$$({\alpha_1}^{3^{sn+1}} - {\alpha_1}^{3^{sn}} + 1) = ({\alpha_1}^3 - \alpha_1 + 1)$$

or

$$({\alpha_1}^{3^{sn}} - \alpha_1)^3 = ({\alpha_1}^{3^{sn}} - \alpha_1).$$

Then ${\alpha_1}^{3^{sn}} - \alpha_1 = \theta \in F_3$, and it is easy to show that

$${\alpha_1}^{3^{ksn}} = \alpha_1 + k\theta. \tag{8}$$

So from (4) and (8) we have

$$\begin{aligned} L_{H_i}(\beta_1) &= \sum_{v=0}^{m_i} t_{iv}((\frac{1}{\alpha_1+2\theta})+(\frac{1}{\alpha_1+\theta})+(\frac{1}{\alpha_1}))^{3^{sv}} \\ &= \sum_{v=0}^{m_i} t_{iv}(\frac{\alpha_1(\alpha_1+\theta)+\alpha_1(\alpha_1+2\theta)+(\alpha_1+2\theta)(\alpha_1+\theta)}{\alpha_1(\alpha_1+\theta)(\alpha_1+2\theta)})^{3^{sv}} \\ &= \sum_{v=0}^{m_i} t_{iv}(\frac{-1}{{\alpha_1}^3-\alpha_1})^{3^{sv}}. \end{aligned}$$

Thus by (6) we have

$$L_{H_i}(\beta_1) = \sum_{v=0}^{m_i} t_{iv}(\frac{\alpha-1}{\alpha})^{3^{sv}} = (\sum_{v=0}^{m_i} t_{iv}(1-\frac{1}{\alpha}))^{3^{sv}}.$$

Denote $P^*(x)$ by $G(x)$, that is N-polynomial. Also it is clear that by theorem's hypothesis and lemma 2.2, $G(-x+1)$ is a N-polynomial. But $1-\frac{1}{\alpha}$ is a root of $G(-x+1)$. Then we have

$$\sum_{v=0}^{m_i} t_{iv}(1-\frac{1}{\alpha})^{3^{sv}} \neq 0$$

and proof is completed.

References

[1] M.Alizadeh, "Contructing Methods for irreducible Polynomials", Mathematical Problems of Computer Scinces, vol. XXXV.2011, PP. 26-32, .

[2] D. Jungnickel, "Trace-Orthogonal normal bases", Discrete applied mathematics, 233-249, 47(1993).

[3] S.Gao."Normal bases over finite fields", Ph.D. Thesis, Waterloo, (1993).

[4] Melsik, k. Kyuregyan. Iterated constructions of irreducible polynomials over finite fields with linearly independent roots. Finite fields and their applications. 10, 323-341(2004).

[5] Melsik, k. Kyuregyan,"Recursive constructions of N-polynomials over $GF(2^s)$", Discrete Applied Mathematics, 156(2008)1554-1559.

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

[7] H.Meyn,"Explicit N-polynomial of 2-power degree over finite fields", Designs, Codes and Cryptography, 6, (1995),147-158

Received: July, 2011