A NOTE ON N-POLYNOMIALS OVER FINITE FIELDS

KITAE KIM AND IKKWON YIE

Abstract. A simple type of Cohen’s transformation consists of a polynomial and a linear fractional transformation. We study the effectiveness of Cohen transformation to find N-polynomials over finite fields.

1. Introduction

Let $F_q$ denote the finite field with $q$ elements, where $q$ is a prime power and $F_q^*$ be its multiplicative group. An element $\alpha$ in an extension $F_{q^n}$ of $F_q$ is called a normal element of $F_{q^n}$ over $F_q$ if its conjugates form a basis of $F_{q^n}$ as an $F_q$-vector space. In this case, the set of conjugates is called a normal basis.

An irreducible polynomial in $F_q[x]$ is called an $N$-polynomial or normal polynomial if its roots are linearly independent over $F_q$. That is, the minimal polynomial of a normal element is $N$-polynomial when conjugates of the normal element form a basis of the splitting field of the minimal polynomial. As in the normal bases, finding criteria and constructing $N$-polynomials is a challenging problem.
Perlis [12] and Pei et al. [11] gave simple normality criteria of polynomials in strictly constrained conditions, which will be presented in section 2. Schwarz [13] proposed a powerful tool for determining whether an irreducible polynomial is an $N$-polynomial, based on vector space argument. Jungnickel [5] proposed several characterizations of self-dual normal bases and their affine transformations, and an explicit construction of a self-dual normal basis in extension fields over $\mathbb{F}_2$. In the paper [8], Kyuregyan suggested an iterated constructions of a sequence $(F_k(x))_{k\geq 1}$ of $N$-polynomials over $\mathbb{F}_2$. The resulting sequence was proven to be trace-compatible in the sense that relative trace $\text{Tr}_{2^n|2^{n-1}}$ maps roots of $F_k(x)$ onto those of $F_{k-1}(x)$. The author also showed that the composition of an $N$-polynomial $F(x)$ and a linear polynomial $ax+b$ remains an $N$-polynomial over $\mathbb{F}_q$ of characteristic $p$ if $\text{deg}(F)$ is divisible by $p$.

In this paper, we revisit Jungnickel’s normality criterion by interpreting in terms of $N$-polynomial, which allows a neat presentation of a result on affine transformation of $N$-polynomials.

2. Preliminaries

Throughout the paper, we assume that $\mathbb{F}_q$ is the finite field with $q$ elements and of characteristic $p$. Note that $p = 2$ is allowed, unless otherwise stated.

**Proposition 2.1** (Cohen [2]). Let $g(x) = \frac{u(x)}{v(x)} \in \mathbb{F}_q(x)$ be a rational function with $\gcd(u, v) = 1$ and let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $n$. Consider the polynomial $F(x)$ defined by

$$F(x) = v^n f\left(\frac{u}{v}\right).$$

Then $F(x)$ is irreducible over $\mathbb{F}_q$ if and only if $u - \alpha v$ is irreducible over $\mathbb{F}_{q^n}$ for some root $\alpha \in \mathbb{F}_{q^n}$ of $f(x)$.

Eq. (1) is referred to Cohen’s transformation. If $f(x)$ is an irreducible polynomial of degree $n$ over $\mathbb{F}_q$ and $g(x)$ is a fractional linear transformation, then $F(x)$ is irreducible over $\mathbb{F}_{q^n}$.

**Proposition 2.2** (Meyn [10]). Let $q = 2^s$ for some positive integer $s$. Let $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ be irreducible of degree $n$. If $\text{Tr}_{q|2}(c_1/c_0) \neq 0$ then $x^n f(x + x^{-1})$ is irreducible over $\mathbb{F}_q$ of degree $2n$. 


Based on above proposition, Gao [3] and Kyuregyan [7] deduced constructions of sequences of irreducible polynomials over \( \mathbb{F}_q \).

**Proposition 2.3 (Kyuregyan [7])**. Let \( \delta \in \mathbb{F}_{2^s}^* \) and \( F_1(x) = \sum_{u=0}^n c_u x^u \) be an irreducible polynomial over \( \mathbb{F}_{2^s} \) whose coefficients satisfy the conditions

\[
\text{Tr}_{2^s} \left( \frac{c_1 \delta}{c_0} \right) = 1 \quad \text{and} \quad \text{Tr}_{2^s} \left( \frac{c_{n-1}}{\delta} \right) = 1.
\]

Then all members of the sequence \( (F_k(x))_{k \geq 1} \) defined by

\[
F_{k+1}(x) = x^{2^k-1} F_k(x + \delta^2 x^{-1}), \quad k \geq 1
\]

are irreducible polynomials over \( \mathbb{F}_{2^s} \).

It was shown that if the initial polynomial \( F_1 \) is given to be an \( N \)-polynomial then the resulting sequence is indeed a family of \( N \)-polynomials [8]. We note that Kyuregyan’s proof of the normality uses the restriction of \( F_1 \) in the above proposition.

**Proposition 2.4 (Perlis [12])**. Let \( n = p^e \) and let \( f = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \) be an irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \). \( f \) is \( N \)-polynomial if and only if \( a_1 \neq 0 \).

### 3. \( N \)-polynomials from Cohen’s transformation

In [5], Jungnickel gives normality criteria of elements on finite fields. The following theorem is an \( N \)-polynomial analogue of Jungnickel’s results on normal elements.

**Theorem 3.1**. Let \( f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \) be a polynomial over \( \mathbb{F}_q \) of degree \( n \geq 1 \) and \( F(x) = f(ax + b) \) where \( a, b \in \mathbb{F}_q \) with \( a \neq 0 \). If \( f(x) \) is an \( N \)-polynomial and \( nba_0 + a_1 \neq 0 \) then \( F(x) \) is an \( N \)-polynomial over \( \mathbb{F}_q \). Conversely, if \( F(x) \) is an \( N \)-polynomial and \( a_1 \neq 0 \) then \( f(x) \) is also an \( N \)-polynomial over \( \mathbb{F}_q \).

**Proof.** First note that, by Proposition 2.1, \( F(x) \) is irreducible over \( \mathbb{F}_q \). Let \( \alpha \) be a root of \( f \). Then

\[
F(x) = a_0 a^n \prod_{i=0}^{n-1} \left( x - \frac{\alpha^i - b}{\alpha} \right).
\]
To prove the first part, it suffices to show that \( \alpha - b, \ldots, \alpha^{q^n-1} - b \) are linearly independent. Suppose that \( \sum_{i=0}^{n-1} c_i(\alpha^{q^i} - b) = 0 \) for \( c_i \in \mathbb{F}_q \). Then, since \( Tr_{q^n/q}(\alpha) = -\frac{a_1}{a_0} \neq 0 \),

\[
\sum_{i=0}^{n-1} c_i \left( -\frac{a_1}{a_0} - nb \right) = 0.
\]

Since \( nba_0 + a_1 \neq 0 \), \( \sum_{i=0}^{n-1} c_i = 0 \) and hence \( \sum_{i=0}^{n-1} c_i \alpha^{q^i} = \sum_{i=0}^{n-1} c_i b = 0 \). Therefore, \( c_i = 0 \) for all \( i \).

Since \( f(x) = F((1/a)x - b/a) \), the second part is an immediate consequence of the first part.

Note that the second highest term of an \( N \)-polynomial is nonzero. The above theorem says that, when \( p \mid n \), \( f(x) \) is an \( N \)-polynomial if and only if \( F(x) \) is an \( N \)-polynomial, which implies the following Kyuregyan’s result:

\[ \text{Corollary 3.2 (Kyuregyan [8])}. \]

Let \( n = p^e n_1 \) with \( \gcd(p, n_1) = 1 \), \( e \geq 1 \). Let \( f(x) = \sum_{i=0}^{n} c_i x^i \) be an \( N \)-polynomial of degree \( n \) over \( \mathbb{F}_q \). If \( a, b \in \mathbb{F}_q \) with \( a \neq 0 \) then the polynomial \( F(x) = f(ax + b) \) is an \( N \)-polynomial over \( \mathbb{F}_q \).

In the study of irreducible polynomials over finite fields, group action has been played an important role. Let \( GL(2, \mathbb{F}_q) \) be the general linear group and \( PGL(2, \mathbb{F}_q) \) the projective linear group defined by the quotient group

\[ PGL(2, \mathbb{F}_q) = GL(2, \mathbb{F}_q)/\{kI_2 \mid k \in \mathbb{F}_q^* \}, \]

where \( I_2 \) denote the \( 2 \times 2 \) identity matrix. Some of \( GL(2, \mathbb{F}_q) \)- and \( PGL(2, \mathbb{F}_q) \)-actions on the set of irreducible polynomials over \( \mathbb{F}_q \) were introduced in literatures. In particular, an action of \( GL(2, \mathbb{F}_q) \) on the set \( \mathcal{M}_n \) of irreducible polynomials over \( \mathbb{F}_q \) of degree \( n \) is given as follows: for a group element \( \sigma \) and an irreducible polynomial \( f \), the \( \sigma \)-action of \( f \) can be given

\[ f^\sigma = (cx + d)^n \cdot f \left( \frac{ax + b}{cx + d} \right), \quad \text{where} \quad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \]

Using equivalence relations on \( GL(2, q) \) and \( \mathcal{M}_n \) given by

\[ \sigma \sim \tau \iff \sigma = \lambda \tau \quad \text{for some} \quad \lambda \in \mathbb{F}_q^*; \]

\[ f \sim g \iff g = \lambda f \quad \text{for some} \quad \lambda \in \mathbb{F}_q^*. \]
A note on N-polynomials over finite fields

A PGL$(2, q)$-action on the set of monic irreducible polynomials is obtained (See [14]). Under the PGL$(2, q)$-action on the set of monic irreducible polynomials, it was shown that if $\gcd(n, q(q^2 - 1)) = 1$ then the point stabilizer is trivial ([1], [14]). That is, $\mathcal{O}_f = \{I_2\}$ for any monic irreducible polynomial $f$.

**Corollary 3.3.** Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be a monic $N$-polynomial of degree $n$ over $\mathbb{F}_q$.

1. If $\gcd(p, n) = 1$, then the compositions $f(x + b)$, for every $b \in \mathbb{F}_q$, produces $(q - 1)$ different monic $N$-polynomials of degree $n$.

2. If $\sigma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in PGL(2, \mathbb{F}_q)$ satisfies $nkb \neq -a_1$ for all $0 \leq k < \text{ord}(\sigma)$, and if $\gcd(n, q(q^2 - 1)) = 1$, then one can get $\text{ord}(\sigma)$ different monic $N$-polynomials over $\mathbb{F}_q$ of degree $n$.

**Proof.** Since $p \nmid n$, there is unique $b \in \mathbb{F}_q$ such that $nb = -a_1$. This means that there are at least $(q - 1)$ number of $N$-polynomials of the form $f(x + b)$ where $b$ satisfies $nb \neq -a_1$. Now, suppose that $f(x + b_1) = f(x + b_2)$ for some $b_1, b_2 \in \mathbb{F}_q$ with $nb_i \neq a_1$ ($i = 1, 2$). Let $\alpha$ be a root of $f(x)$. Then

$$\sum_{i=0}^{n} b_1 - \alpha^{q^i} = \sum_{i=0}^{n} b_2 - \alpha^{q^i}.$$ 

That is, $nb_1 = nb_2$. Since $p \nmid n, b_1 = b_2$. Therefore, such $N$-polynomials of the form $f(x + b)$ must be distinct, and this proves the first part.

For each $k$,

$$\sigma^k = \begin{pmatrix} 1 & kb \\ 0 & 1 \end{pmatrix}.$$ 

By Theorem 3.1 and the assumption $nkb + a_1 \neq 0$, we conclude $f^{\sigma^k}$ are $N$-polynomials for all $k$, and the second part follows from the argument mentioned above. \hfill $\square$

It seems hard to get normality criteria for such actions in full generality. On the other hand, we suggest a condition for an element $\sigma$ of $GL(2, q)$ or $PGL(2, q)$ to preserve the normality of polynomials whose degrees are power of characteristic $p$.

**Theorem 3.4.** Let $n = p^e$ with $e \geq 1$ and $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q)$. Let $f(x)$ be an $N$-polynomial of degree $n$ and $\alpha$ a root of $f$. If $\text{Tr}_{q^e|q}(\frac{\alpha}{c\alpha - a})$
≠ 0 then $f^\sigma$ is an $N$-polynomial of degree $n$. In case that $a ≠ 0$, it is an equivalent condition.

Proof. Let $a_n$ denote the leading coefficient of $f(x)$, and write $f^\sigma$ as

$$a_n \left[ \prod_i (a - c\alpha^q) \right] \left[ \prod_i \left( x + \frac{b - d\alpha^q}{a - c\alpha^q} \right) \right].$$

Let $\beta = \frac{-da + b}{ca - a}$. Since $p | n$, we have $Tr_{q^n|q}(\alpha(c\beta + d)) = Tr_{q^n|q}(a\beta)$.

Since

$$c\beta + d = c\frac{-da + b}{ca - a} + d = \frac{-cd\alpha + cb + cda - ad}{ca - a} = \frac{-ad + bc}{ca - a},$$

$$(-ad + bc) Tr_{q^n|q} \left( \frac{\alpha}{ca - a} \right) = a Tr_{q^n|q}(\beta). \quad (2)$$

Note that, by Proposition 2.1, $f^\sigma$ is irreducible. Hence, Proposition 2.4 tells us that $f^\sigma$ is $N$-polynomial if and only if $Tr_{q^n|q}(\beta) ≠ 0$. Therefore, the assertion follows immediately from Eq. (2). \qed

4. $N$-polynomials from Q-transformation

In this section, we assume $\mathbb{F}_q$ is a finite field of characteristic 2 and $f(x)$ is a polynomial of degree $n$ over $\mathbb{F}_q$. The $Q$-transformation of $f$ is defined by

$$f^Q(x) := x^n f(x + \delta^2 x^{-1}),$$

where $\delta \in \mathbb{F}_q^*$. Based on Proposition 2.3, M.K. Kyuregyan established an infinite sequence of $N$-polynomials over $\mathbb{F}_q$ ([8], see Corollary 4.2 below). Kyuregyan’s proof for normality of resulting sequences depends on initial conditions (see Eq. (3) below). In this section, we give a slightly different presentation of Kyuregyan’s proof without initial conditions.
Lemma 4.1. Let \( f(x) \) be an \( N \)-polynomial over \( \mathbb{F}_q \) of degree \( n \), and \( \eta, \gamma \in \mathbb{F}_q^* \). Let \( F(x) \) be a polynomial defined by
\[
F(x) = x^n f(\eta x + \frac{\gamma}{x}).
\]
If \( F(x) \) is irreducible over \( \mathbb{F}_q \) then it is an \( N \)-polynomial of degree \( 2n \).

Proof. We first write \( f(x) \) as
\[
f(x) = a_0 \prod_{i=0}^{n-1} (x - \alpha^{q^i}).
\]
Then
\[
F(x) = a_0 x^n \prod_{i=0}^{n-1} (\eta x + \frac{\gamma}{x} - \alpha^{q^i})
= a_0 x^n \prod_{i=0}^{n-1} \left( x^2 - \frac{1}{\eta} \alpha^{q^i} x + \frac{\gamma}{\eta} \right).
\]
Note that, since \( F(x) \) is irreducible over \( \mathbb{F}_q \), \( x^2 - \frac{1}{\eta} \alpha^{q^i} x + \frac{\gamma}{\eta} \) will be irreducible over \( \mathbb{F}_{q^n} \) for each \( 0 \leq i < n \). Let \( \beta \) be a root of \( x^2 - \frac{1}{\eta} \alpha^{q^i} x + \frac{\gamma}{\eta} \). Then \( \alpha = \beta + \beta^{q^n} \). Suppose that \( \sum_{i=0}^{2n-1} c_i \beta^{q^i} = 0 \) for \( c_i \in \mathbb{F}_q \). Then \( \sum_{i=0}^{2n-1} c_i \beta^{q^i+1} = 0 \) and so \( \sum_{i=0}^{2n-1} c_i \alpha^{q^i} = 0 \), for \( \alpha = \beta + \beta^{q^n} \). Since \( f(x) \) is an \( N \)-polynomial over \( \mathbb{F}_q \) of degree \( n \), \( \alpha, \ldots, \alpha^{q^n} \) form a normal basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \), and hence \( c_{n+i} = c_i \) for each \( 0 \leq i < n \). Thus, we get
\[
0 = \sum_{i=0}^{2n-1} c_i \beta^{q^i} = \sum_{i=0}^{n-1} c_i \beta^{q^i} + \sum_{i=0}^{n-1} c_i \beta^{q^{n+i}}
= \sum_{i=0}^{n-1} c_i (\beta^{q^i} + \beta^{q^{n+i}}) = \sum_{i=0}^{n-1} \frac{c_i}{\eta} \alpha^{q^i}.
\]
Since \( \alpha, \ldots, \alpha^{q^{n-1}} \) are linearly independent over \( \mathbb{F}_q \), we have \( c_i = 0 \) for \( 0 \leq i < n \). Therefore, \( c_i = 0 \) for all \( 0 \leq i < 2n \). That is, \( F(x) \) must be an \( N \)-polynomial over \( \mathbb{F}_q \).

In above proof, \( \alpha \) and \( \beta \) satisfy \( \alpha = \beta + \beta^{q^n} \), and so \( Tr_{q^{2n}|q^n}(\beta) = \alpha \). That is, \( f(x) \) and \( F(x) \) are trace-comparable.
Corollary 4.2 (Kyuregyan [8]). Let $s$ be a positive integer, $\delta \in \mathbb{F}_2^*$ and $F_1(x) = \sum_{u=0}^{n} c_u x^u$ be an $N$-polynomial of degree $n$ over $\mathbb{F}_2^*$ such that

\begin{equation}
Tr_{2^s}|_2 \left( \frac{c_1 \delta}{c_0} \right) = 1 \quad \text{and} \quad Tr_{2^s}|_2 \left( \frac{c_{n-1}}{\delta} \right) = 1.
\end{equation}

Then the sequence $(F_k(x))_{k \geq 1}$ defined by

$$F_{k+1}(x) = x^{2^{k-1}n} F_k(x + \delta^2 x^{-1}), \quad k \geq 1$$

is a trace-compatible sequence of $N$-polynomials of degree $2^k n$ over $\mathbb{F}_2^*$ for every $k \geq 1$.

Proof. By Proposition 2.3, it suffices to prove the normality of the sequence. For each $k \geq 1$, applying Theorem 4.1 recursively with $q = 2^s, n = 2^k n, \eta = 1, \gamma = \delta^2, f(x) = F_k(x)$ yields that $F_{k+1}$ is an $N$-polynomial of degree $2^k n$ over $\mathbb{F}_2^*$.

We remark that Lemma 4.1 can be deduced from Corollary 4.2 by taking $k = 1$ and using suitable transformation.

Corollary 4.3. Let $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_2^*[x]$ be an $N$-polynomial of degree $n$. If $Tr_{2^s}|_2(c_1/c_0) \neq 0$ then $x^n f(x + x^{-1})$ is an $N$-polynomial over $\mathbb{F}_2^*$ of degree $2n$.

Proof. By Proposition 2.2, $x^n f(x + x^{-1})$ is irreducible over $\mathbb{F}_2^*$. Hence, the result follows by taking taking $\eta = \gamma = 1$ in Theorem 4.1, we obtain the desired result.

References


Kitae Kim  
Department of Mathematics, Inha University  
Incheon, Korea  
E-mail: ktkim@inha.ac.kr

Ikkwon Yie  
Department of Mathematics, Inha University  
Incheon, Korea  
E-mail: ikyie@inha.ac.kr