Korean J. Math. **28** (2020), No. 3, pp. 639–647
http://dx.doi.org/10.11568/kjm.2020.28.3.639

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

An irreducible polynomial in $\mathbb{F}_q[x]$ is called an *N-polynomial* or *normal polynomial* if its roots are linearly independent over $\mathbb{F}_q$. 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.

Received July 28, 2020. Revised September 8, 2020. Accepted September 18, 2020.

2010 Mathematics Subject Classification: 11T71, 12E10, 12E20.

Key words and phrases: Normal basis, N-polynomial, Cohen transformation, Q-transormation.

This research was supported by the National Research Foundation of Korea grant funded by the Korea government (NRF-2017R1D1A1B03034721).

Perlis [12] and Pei et al. [11] gave simple normaility 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-polynomia, 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 $\mathbb{F}_{2^s}$. The resulting sequence was proven to be *trace-compatible* in the sense that relative trace $Tr_{2^k n|2^{k-1}n}$ 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 $\deg(F)$ 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*

$$F(x) \;=\; v^n f\left(\frac{u}{v}\right). \tag{1}$$

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 $f(x)=\sum_{i=0}^{n}c_ix^i\in\mathbb{F}_q[x]$ be irreducible of degree n. If $Tr_{q|2}(c_1/c_0)\neq 0$ then $x^nf(x+x^{-1})$ 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*

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

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

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

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 α be a root of f. Then

$$F(x) \quad = \quad a_0 a^n \prod_{i=0}^{n-1} \left(x - \frac{\alpha^{q^i} - b}{a} \right).$$

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:

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 2×2 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 σ and an irreducible polynomial f, the σ-action of f can be given

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

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

$$\sigma \sim \tau \Leftrightarrow \sigma = \lambda\tau \quad \text{for some } \lambda \in \mathbb{F}_q^*;$$
$$f \sim g \Leftrightarrow g = \lambda f \quad \text{for some } \lambda \in \mathbb{F}_q^*,$$

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 $0 \leq k < ord(\sigma)$, and if $\gcd(n, q(q^2-1)) = 1$, then one can get $ord(\sigma)$ 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 α 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^{σ^k} are N-polynomials for all k, and the second part follows from the argument mentioned above. □

It seems hard to get normality criteria for such actions in full generality. On the other hand, we suggest a condition for an element σ 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 α a root of f. If $Tr_{q^n|q}(\frac{\alpha}{c\alpha - a})$*

$\neq 0$ then f^σ is an N-polynomial of degree n. In case that $a \neq 0$, it is an equivalent condition.

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

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

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

$$\begin{aligned} c\beta + d &= c\frac{-d\alpha + b}{c\alpha - a} + d \\ &= \frac{-cd\alpha + cb + cd\alpha - ad}{c\alpha - a} \\ &= \frac{-ad + bc}{c\alpha - a}, \end{aligned}$$

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

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

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 Corollaryollary 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

$$\begin{aligned} F(x) &= a_0 x^n \prod_{i=0}^{n-1} (\eta x + \frac{\gamma}{x} - \alpha^{q^i}) \\ &= a_0 \eta^n \prod_{i=0}^{n-1} (x^2 - \frac{1}{\eta}\alpha^{q^i} x + \frac{\gamma}{\eta}). \end{aligned}$$

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 $0 \le i < n$. Let β be a root of $x^2 - \frac{1}{\eta}\alpha x + \frac{\gamma}{\eta}$. 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 $0 \le i < n$. Thus, we get

$$\begin{aligned} 0 &= \sum_{i=0}^{2n-1} c_i \beta^{q^i} = \sum_{i=0}^{n-1} c_i \beta^{q^i} + \sum_{i=0}^{n-1} c_i \beta^{q^{n+i}} \\ &= \sum_{i=0}^{n-1} c_i (\beta^{q^i} + \beta^{q^{n+i}}) = \sum_{i=0}^{n-1} \frac{c_i}{\eta} \alpha^{q^i}. \end{aligned}$$

Since $\alpha, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$, we have $c_i = 0$ for $0 \le i < n$. Therefore, $c_i = 0$ for all $0 \le i < 2n$. That is, $F(x)$ must be an N-polynomial over $\mathbb{F}_q$. $\square$

In above proof, α and β 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, $\delta \in \mathbb{F}_{2^s}^*$ and $F_1(x) = \sum_{u=0}^{n} c_u x^u$ be an N-polynomial of degree n over $\mathbb{F}_{2^s}$ such that*

$$Tr_{2^s|2}\left(\frac{c_1\delta}{c_0}\right) = 1 \quad \text{and} \quad Tr_{2^s|2}\left(\frac{c_{n-1}}{\delta}\right) = 1. \tag{3}$$

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 $\mathbb{F}_{2^s}$ 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 $\mathbb{F}_{2^s}$. □

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 $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_{2^s}[x]$ 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 $\mathbb{F}_{2^s}$ of degree $2n$.*

Proof. By Proposition 2.2, $x^n f(x+x^{-1})$ is irreducible over $\mathbb{F}_{2^s}$. Hence, the result follows by taking taking $\eta = \gamma = 1$ in Theorem 4.1, we obtain the desired result. □

References

[1] X. Cao and L. Hu, *On the reducibility of some composite polynomials over finite fields*, Des. Codes Cryptogr. **64** (2012), 229–239.

[2] S. D. Cohen, *The explicit construction of irreducible polynomials over finite fields*, Des. Codes Cryptogr. **2** (1993), 169–173.

[3] S. Gao, *Normal bases over finite fields*, PhD Thesis, Univ. of Waterloo, Canada, 1993.

[4] Garefalskis, *On the action of $GL_2(\mathbb{F}_q)$ of irreducible polynomials over finite fields*, J. Pure Appl. Algebra **215**(2011), 159–176.

[5] D. Jungnickel, *Trace-orthogonal normal bases*, Discrete Appl. Math. **47** (1993) 233–249.

[6] K. Kim, J. Namgoong, I. Yie, *Groups of permutations generated by function–linear translator pairs*, Finite Fields Appl. **45** (2017) 170–182.

[7] M.K. Kyuregyan, *Recurrent methods for constructing irreducible polynomials over* $GF(2^s)$, Finite Fields Appl. **8** (2002), 52–68.

[8] M.K. Kyuregyan, *Iterated constructions of irreducible polynomials over finite fields with linearly independent roots*, Finite Fields Appl. **10** (2004), 323–341.

[9] A. Lempel and M. J. Weinberger, *Self-complementary normal bases in finite fields*, SIAM J. Discrete Math. **1** (1988), 758–767.

[10] H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, App. Alg in Eng., Comm. and Comp. **1** (1990), 43–53.

[11] D. Pei, C.C. Wang and J.K. Omura, *Normal bases of finite field* $GF(2^m)$*"* IEEE Trans. Info. Th. **32** (1986), 285–287.

[12] S. Perlis, *Normal bases of cyclic fields of prime-power degree*, Duke Math. J. 9 (1942), 507-517.

[13] S.S. Schwarz, "Construction of normal bases in cyclic extensions of a field", Czechslovak Math. J. 38(1988), 291-312.

[14] H. Stichtenoth and A. Topouzoglu, *Factorization of a class of polynomials over finite fields*, Finite Fields Appl. 18 (2012), 108-122.

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