Mathematical Problems of Computer Science 23, 2004, 59–66.

Construction of Sequences of N-polynomials Over Finite Fields of Odd Characteristics

Gevorg M. Hambardzumyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail gev@hylink.am

Abstract

In this paper the method of construction of N-polynomials over F_q with $q \equiv 1 \pmod 4$ is presented. For a suitably chosen initial N-polynomial $f_1(x) \in F_q[x]$ of degree 2 N-polynomials $f_k(x) \in F_q[x]$ of degree 2^k are constructed by the iterated application of following transformation: $f(x) \to (2x)^{\deg(f)} f\left(\frac{x+\eta^2 x^{-1}}{2}\right), \eta \in F_q, \eta \neq 0$.

1 Introduction

In this paper we use a method similar to Meyn's [3] to show that Kyuregyan's [2] construction gives a more general iterative technique to construct sequences of polynomials of degrees 2^k over F_q compared to one given by Meyn, which was based on the Cohen's [1] result.

Let F_q be the Galois field of order $p = q^s$ where p is an odd prime and s is a natural number. Let $f(x)$ be a monic irreducible polynomial of degree n over F_q and β its root. The field F_{q^n} is an extension of F_q and can be considered as a vector space of dimension n over F_q.

A normal basis of F_{q^n} over F_q is a basis of form $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$, i.e. a basis consisting of all the algebraic conjugates of α. We say that α generates normal basis, or α is a normal element of F_{q^n} over F_q.

A monic irreducible polynomial $f(x) \in F_q[x]$ is called normal or N-polynomial if its roots are linearly independent over F_q. The elements in a normal basis are exactly the roots of some N-polynomial. Hence, an N-polynomial is just another way of describing a normal basis.

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

We briefly recapitulate some concepts from linear algebra. Let T be a linear transformation on a finite-dimensional vector space V over an arbitrary field F. A subspace $W \subseteq V$ is called T-invariant if $\forall u \in W, Tu \in W$. For any vector $u \in V$, the subspace spanned by $u, uT, uT^2, \ldots$ is T-invariant and called the T-cyclic subspace generated by u. Denote it $Z(u,T)$. $Z(u,T)$ consists of all vectors of the form $g(T)u, g(x) \in F$. If $Z(u,T) = V$, then u is called a cyclic vector of V for T.

For any polynomial $g(x) \in F[x]$, $g(T)$ is a linear transformation on V. The null space of $g(T)$ consists of all vectors u such that $g(T)u = 0$. We also call it null space of $g(x)$. On the other hand, for any vector $u \in V$ the monic polynomial $g(x) \in F[x]$ of smallest degree such that $g(T)u = 0$ is called the T-order of u (some authors call it the T-annihilator, minimal polynomial of u or additive order of u). Denote this polynomial by $Ord_{u,T}(x)$, or $Ord_u(x)$ if the transformation T is clear from context. Note that $Ord_u(x)$ divides any polynomial annihilating u.

Recall that the Frobenius map

$$\sigma : \gamma \to \gamma_q,\ \gamma \in F_{q^n}$$

is an automorphism of F_{q^n} that fixes F_q. In particular, σ is a linear transformation of F_{q^n} viewed as a vector space of dimension n over F_q. It is well known fact that the minimal and characteristic polynomials for σ are identical both being $x^n - 1$. By definition, α is a normal element if and only if $\alpha,\ \sigma\alpha,\ \sigma^2\alpha,\ \ldots,\ \sigma^{n-1}\alpha$ are linearly independent over F_{q^n}(α is a cyclic vector of F_{q^n} for σ). If $\alpha \in F_{q^n}$ is a normal element then there is no polynomial of degree less than n that annihilates α. So it follows that α is a normal element if and only if $Ord_{\alpha,\sigma} = x^n - 1$. For any polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

define

$$f \circ \alpha = \sum_{i=0}^{n} a_i \sigma^i \alpha = \sum_{i=0}^{n} a_i \alpha^{q^i}.$$

2 N-polynomials and quadratic extensions

We consider certain infinite extensions of a finite field F_q, which have the shape

$$F_{q^{2^\infty}} = \bigcup_{k \geq 0} F_{q^{2^k}},\ q \equiv 1 \pmod 4$$

and are specified by a sequence of irreducible polynomials $f_k(x) \in F_q[x]$ of degrees 2^k. For suitable chosen initial N-polynomial $f_1(x) \in F_q[x]$ of degree 2, the defining N-polynomials $f_k(x) \in F_q[x]$ of degree 2^k are constructed by the iterated application of following transformation:

$$f(x) \to (2x)^{\deg f(x)} f\left(\frac{x + \eta^2 x^{-1}}{2}\right) \tag{1}$$

For more general transformation Kyuregyan[2] proved that it generates the sequence of irreducible polynomials:

Theorem 1. (Kyuregyan [2]) *Let $P(x) \neq x$ be an irreducible polynomial of degree $n \geq 1$ over F_q where n is even if $q \equiv 3 \pmod 4), r, h, \delta \in F_q$ and $r \neq 0, \delta \neq 0$. Suppose that $P\left(\frac{2\delta - rh}{r^2}\right) P\left(-\frac{2\delta + rh}{r^2}\right)$ is a non-square in F_q. Define*

$$F_0(x) = P(x),$$

$$F_k(x) = \left(2x + \frac{2h}{r}\right)^{t_{k-1}} F_{k-1}\left(\left(x^2 + \frac{4\delta^2 - (hr)^2}{r^4}\right) / \left(2x + \frac{2h}{r}\right)\right) \tag{2}$$

where $t_k = n2^k$ denotes the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over F_q of degree $n2^k$ for every $k \geq 1$.

Here we show that for $h = 0$ in Theorem 1 sequence (2) is a sequence of N-polynomials.

Theorem 2. *Let $q \equiv 1 \pmod 4$ be a prime power and $f_1 \in F_q[x]$ be a monic self-reciprocal N-polynomial of degree 2 such that $f_1(\eta) f_1(-\eta)$ is a nonsquare in F_q, where $\eta \in F_q$, $\eta \neq 0$. Then the sequence $f_k(x)_{k\geq 1}$ defined by*

$$f_{k+1} = (2x)^{2^k} f_k\left(\frac{x+\eta^2 x^{-1}}{2}\right) \tag{3}$$

consists entirely of N-polynomials.

According to Theorem 1 any sequence $f_k(x)_{k\geq 1}$ satisfying (3) will define a sequence of extension fields K_k isomorphic to F_{q^k}. For $k \geq 0$ the 2^k-th power of Frobenius automorphism, i.e. $\gamma \to \gamma^{q^{2^k}}$, will be denoted by σ_k. Note that this notation implies $\sigma_k{}^2 = \sigma_{k+1}$. The roots $\alpha_k \in K_k$ of f_k can be arranged in such a way that

$$\alpha_{k+1} + \eta^2 \alpha_{k+1}^{-1} = 2\alpha_k,\ k \geq 1 \tag{4}$$

Then by applying σ_k to (4) and subtracting (4) from that we get

$$\sigma_k\alpha_{k+1} + \eta^2\sigma_k\alpha_{k+1}^{-1} - \alpha_{k+1} - \eta^2\alpha_{k+1}^{-1} = 0$$

$\sigma_k\alpha_{k+1}+\eta^2\sigma_k\alpha_{k+1}^{-1}-\alpha_{k+1}-\eta^2\alpha_{k+1}^{-1} = \sigma_k\alpha_{k+1}-\eta^2\alpha_{k+1}^{-1}-\left(\alpha_{k+1} - \eta^2\sigma_k\alpha_{k+1}^{-1}\right) = \left(\alpha_{k+1}\sigma_k\alpha_{k+1} - \eta^2\right)\alpha_{k\cdot}^{-}$
$\left(\alpha_{k+1}\sigma_k\alpha_{k+1} - \eta^2\right)\sigma_k\alpha_{k+1}^{-1} =$
$\left(\alpha_{k+1}\sigma_k\alpha_{k+1} - \eta^2\right)\left(\alpha_{k+1}^{-1} - \sigma_k\alpha_{k+1}^{-1}\right) = 0$
$\left(\alpha_{k+1}^{-1} - \sigma_k\alpha_{k+1}^{-1}\right) \neq 0 \Rightarrow \left(\alpha_{k+1}\sigma_k\alpha_{k+1} - \eta^2\right) = 0$
So we get

$$\sigma_k\alpha_{k+1} = \eta^2\alpha_{k+1} \tag{5}$$

and

$$Tr_{K_{k+1}/K_k}(\alpha_{k+1}) = \alpha_{k+1} + \sigma_k\alpha_{k+1} = \alpha_{k+1} + \eta^2\alpha_{k+1}^{-1} = 2\alpha_k \tag{6}$$

We shall proof by induction on k that α_k generates a normal basis over $K_0 = F_q$. By construction, the starting polynomial f_1 is an N-polynomial, i.e. α_1 generates a normal basis of K_1/K_0. Suppose by induction that

$$Ord_{\alpha_k}(x) = x^{2^k} - 1. \tag{7}$$

We have to proof that $Ord_{\alpha_{k+1}}(x) = x^{2^{k+1}} - 1$. The relation (6) shows that

$$Tr_{K_{k+1}/K_k}(\alpha_{k+1} - \alpha_k) = 2\alpha_k - 2\alpha_k = 0 \tag{8}$$

Following Meyn [3] we now denote

$$\beta_{k+1} := \alpha_{k+1} - \alpha_k \tag{9}$$

These differences are non-zero, by Theorem 1, and

$$\sigma_k\beta_{k+1} = \sigma_k\alpha_{k+1} - \alpha_k = \eta^2\alpha_{k+1}^{-1} = 2\alpha_k - \alpha_{k+1} - \alpha_k = \alpha_k - \alpha_{k+1}$$

$$\sigma_k\beta_{k+1} = -\beta_{k+1} \tag{10}$$

As β_{k+1} has trace zero we know that $Ord_{\beta_{k+1}}(x)$ is a divisor of $x^{n+1}-1$. On the other hand $\alpha_{k+1}=\alpha_k+\beta_{k+1}$ is the sum of two elements of relatively prime additive orders so that the additive order of α_{k+1} is the product of $x^k-1=Ord_{\alpha_k}(x)$ and the additive order of β_{k+1}. By this, we have the equivalence

$$Ord_{\alpha_{k+1}}(x)=x^{2^k}+1 \Leftrightarrow Ord_{\beta_{k+1}}(x)=x^k-1.$$

Remarkably, the fact that $Ord_{\beta_{k+1}}(x)$ is equal to $x^{2^k}+1$ will be proved without further use of induction hypothesis (7). By substituting (5) and (6) in (9) we get:

$$\beta_{k+1}=\alpha_{k+1}-(\alpha_{k+1}+\sigma_k\alpha_{k+1})/2=\alpha_{k+1}/2-\sigma_k\alpha_{k+1}/2$$

So elements β_{k+1} have the following representation:

$$\beta_{k+1}=\alpha_{k+1}/2-\sigma_k\alpha_{k+1}/2 \tag{11}$$

The following relations between elements also take place:

$$\beta_{k+1}^2=\alpha_{k+1}^2-2\alpha_{k+1}\alpha_k+\alpha_k^2=\alpha_k^2-\alpha_{k+1}(2\alpha_k-\alpha_{k+1})=\alpha_k^2-\alpha_{k+1}\eta^2\alpha_{k+1}^{-1}=\alpha_k^2-\eta^2=$$
$$\alpha_k\left(\alpha_k-\eta^2\alpha_k^{-1}\right)=\alpha_k(\alpha_k-\sigma\alpha_k)=\alpha_k 2\beta_k$$

So we get:

$$\beta_{k+1}^2=\alpha_k^2-\eta^2=2\alpha_k\beta_k \tag{12}$$

Also

$$(\alpha_{k+1}\pm\eta)^2=\alpha_{k+1}\left(\alpha_{k+1}\pm 2\eta+\eta^2/\alpha_{k+1}\right)=\alpha_{k+1}(2\alpha_k\pm 2\eta)=2\alpha_{k+1}(\alpha_k\pm\eta)$$

$$(\alpha_{k+1}\pm\eta)^2=2\alpha_{k+1}(\alpha_k\pm\eta) \tag{13}$$

According to the test we restate problem we got to deal with: Is it true that for any irreducible factor $h(x)$ of $x^{2^k}+1$

$$\frac{x^{2^k}+1}{h(x)}\circ\beta_{k+1}\neq 0 \tag{14}$$

Now we need information about factorization of the 2^{k+1}-st cyclotomic polynomial $x^{2^k}+1$.

Proposition 1. *Let $q\equiv 1 \pmod 4$, i.e. $q=2^A m+1$, $A\geq 1$, m is odd. Define $d=d(k)=\max\{k+1-A,0\}$. Then $x^{2^k}+1$ splits into the product of 2^{k-d} irreducible binomials over F_q:*

$$x^{2^k}+1=\prod_{u\in U}\left(x^{2^d}-u\right),$$

where $U\subset F_q$ is the set of all primitive 2^{k+1-d}th roots of unity.

Proof. See[3].

For fixed A and increasing k the number of factors is equal to 2^{k-d} as long as $k\leq A-1$ and is equal to 2^{A-1} for all $k\geq A-1$. In particular beginning with $k=A-1$ all 2^Ath primitive roots of unity in F_q are used in factorization.

We fix one of these roots, say r, and write the quotient in (14) in the following way:

$$\frac{x^{2^k}+1}{h(x)}=\frac{x^{2^k}+1}{x^{2^d}-r}=\left(x^{2^d}+r\right)\left(x^{2^{d+1}}+r^2\right)\ldots\left(x^{2^{k-1}}+r^{2^{k-d-1}}\right)=\prod_{j=0}^{k-d}\left(x^{2^{k-j}}+r^{2^{k-d-j}}\right)$$

Now we define the images of the partial product of this expansion: $\beta_{k+1}^{(0)} := \beta_{k+1}$ and for $1 \le i \le k-d$

$$\beta_{k+1}^{(i)} := \left(\prod_{l=1}^{i}\left(x^{2^{k-l}} + r^{2^{k-d-l}}\right)\right) \circ \beta_{k+1}$$

which recursively reads:

$$\beta_{k+1}^{(i)} = \left(x^{2^{k-i}} + r^{2^{k-d-i}}\right) \circ \beta_{k+1}^{(i-1)} \tag{15}$$

In this setting problem (14) is

$$\beta_{k+1}^{(k-d)} \neq 0 \quad ?$$

This is obviously equivalent to:

$$\beta_{k+1}^{(i)} \neq 0, \quad 1 \le i \le k-d \tag{16}$$

Based on the results obtained by Meyn[3], we suggest a more general result:

Lemma 1. *The elements satisfy for all $1 \le i \le k-d-1$:*

(a)$\sigma_{k-i-1}\beta_{k+1}^{(i)} = \zeta^{(i)} \cdot \eta \cdot \beta_{k+1}^{(i)}/\alpha_{k-i}$, where the primitive 2^{i+2}nd root of unity $\zeta^{(i)} = \pm r^{2^{k-d-i-1}}$, and

(b) $\left(\beta_{k+1}^{(i)}\right)^{2^{i+1}} = 2^{c(i)} \cdot \beta_{k-i} \cdot \alpha_{k-i}^{2^i} \cdot (\alpha_{k-i-1} \pm \eta)^{2^i-1}$, where $c(i)$ is a certain exponentially increasing function of i.

Proof. We will proof this lemma by induction on i.

$i = 0$. By (12) we have $\beta_{k+1}^2 = 2\alpha_k\beta_k$ so that $c(0) = 1$. Further from (6) and (11) we find $\sigma_{k-1}\beta_{k+1}^2 = -2 \cdot \eta^2 \cdot \beta_k/\alpha_k$ and the quotient $\sigma_{k-1}\beta_{k+1}^2/\beta_{k+1}^2 = -\eta^2/\alpha^2$. It follows that $\sigma_{k-1}\beta_{k+1} = \zeta^{(0)} \cdot \eta \cdot \beta_{k+1}/\alpha_k$, where $\zeta^{(0)}$ is one of two primitive 4-th roots of unity, i.e. $\zeta^{(0)} = \pm r^{2^{k-d-1}}$. The strategy for the induction step is as follows: we have to square the element $\beta_{k+1}^{(i)}$ $i+1$ times in total which will be done in portions $1 + (i-1) + 1$. The first squaring gives a relation between $\left(\beta_{k+1}^{(i)}\right)^2$ and $\left(\beta_{k+1}^{(i-1)}\right)^2$. After squaring another $i-1$ times we are in position to apply induction hypothesis (b). By squaring for a last time, the induction for (b) is complete and the action of automorphism σ_{k-i-1} becomes computable. In the end, all these squarings prove to be reversible with (a). $i : 0 \to 1$

$$\left(\beta_{k+1}^{(1)}\right)^2 = \left(\sigma_{k-1}\beta_{k+1} + r^{2^{k-d-1}}\beta_{k+1}\right)^2 = \beta_{k+1}^2 \cdot r^{2^{k-d}} \cdot (1 \pm \eta/\alpha_k)^2 =$$

$$\beta_{k+1}^2 \cdot r^{2^{k-d}} \cdot \alpha_k^{-2} \cdot (\alpha_k \pm \eta)^2 = \beta_{k+1}^2 \cdot r^{2^{k-d}} \cdot \alpha_k^{-1} \cdot 2 \cdot (\alpha_{k-1} \pm \eta) =$$

$$2 \cdot \beta_k \cdot \alpha_k \cdot r^{2^{k-d}} \cdot \alpha_k^{-1} \cdot 2 \cdot (\alpha_{k-1} \pm \eta) = 2^2 \cdot \beta_k \cdot r^{2^{k-d}} \cdot (\alpha_{k-1} \pm \eta)$$

$$\left(\beta_{k+1}^{(1)}\right)^{2^2} = 2^4 \cdot \beta_k^2 \cdot r^{2^{k-d+1}} \cdot 2 \cdot \alpha_{k-1} \cdot (\alpha_{k-2} \pm \eta) = 2^4 \cdot 2 \cdot \beta_{k-1}\alpha_{k-1} \cdot r^{2^{k-d+1}} \cdot 2 \cdot \alpha_{k-1} \cdot (\alpha_{k-2} \pm \eta) =$$

$$2^{c(1)} \cdot \beta_{k-1} \cdot \alpha_{k-1}^2 \cdot (\alpha_{k-2} \pm \eta)$$

$$\frac{\sigma_{k-2}\left(\beta_{k+1}^{(1)}\right)^{2^2}}{\left(\beta_{k+1}^{(1)}\right)^{2^2}} = \frac{\sigma_{k-2}\beta_{k-1} \cdot \sigma_{k-2}\alpha_{k-1}^2}{\beta_{k-1} \cdot \alpha_{k-1}^2} = \frac{(-\beta_{k-1}) \cdot \left(\eta^2 \cdot \alpha_{k-1}^{-1}\right)^2}{\beta_{k-1} \cdot \alpha_{k-1}^2} = (-1) \cdot \eta^4 \cdot \alpha_{k-1}^{-4}$$

By taking 4th root from this we get

$$\sigma_{k-2}\beta_{k+1}^{(1)} = \zeta^{(1)} \cdot \eta \cdot \beta_{k+1}^{(1)}/\alpha_{k-1},$$

where $\zeta^{(1)}$ is the 2^3rd primitive root of unity.
$i : 1 \to 2$

$$\left(\beta^{(2)}_{k+1}\right)^2 = \left(\sigma_{k-1}\beta^{(1)}_{k+1} + r^{2^{k-d-2}}\beta^{(1)}_{k+1}\right)^2$$

From previous step we have $\sigma_{k-2}\beta^{(1)}_{k+1} = \zeta^{(1)} \cdot \eta \cdot \beta^{(1)}_{k+1}/\alpha_{k-1}$, so that

$$\left(\beta^{(2)}_{k+1}\right)^2 = \left(\sigma_{k-1}\beta^{(1)}_{k+1} + r^{2^{k-d-2}} \cdot \beta^{(1)}_{k+1}\right)^2 = \left(\left(\pm r^{2^{k-d-2}}\right) \cdot \eta \cdot \beta^{(1)}_{k+1}/\alpha_{k-1} + r^{2^{k-d-2}} \cdot \beta^{(1)}_{k+1}\right)^2 =$$

$$\left(\beta^{(1)}_{k+1}\right)^2 \cdot r^{2^{k-d-1}} \cdot \alpha^{-2}_{k-1} \cdot (\alpha_{k-1} \pm \eta)^2 = \left(\beta^{(1)}_{k+1}\right)^2 \cdot r^{2^{k-d-1}} \cdot \alpha^{-1}_{k-1} \cdot 2 \cdot (\alpha_{k-2} \pm \eta) =$$

$$\left(\beta^{(2)}_{k+1}\right)^{2^2} = \left(\beta^{(1)}_{k+1}\right)^{2^2} \cdot r^{2^{k-d}} \cdot \alpha^{-2}_{k-1} \cdot 2^2 \cdot (\alpha_{k-2} \pm \eta)^2 =$$

$$2^{c(1)} \cdot \beta_{k-1} \cdot \alpha^2_{k-1} \cdot (\alpha_{k-2} \pm \eta) \cdot (-1) \cdot \alpha^{-2}_{k-1} \cdot 2^2 \cdot (\alpha_{k-2} \pm \eta)^2 = (-1) \cdot 2^{c(1)} \cdot 2^2 \cdot \beta_{k-1} \cdot (\alpha_{k-2} \pm \eta)^3$$

$$\left(\beta^{(2)}_{k+1}\right)^{2^3} = 2^{2c(1)} \cdot 2^{2^2} \cdot \beta^2_{k-1} \cdot \left((\alpha_{k-2} \pm \eta)^2\right)^3 = 2^{2c(1)} \cdot 2^{2^2} \cdot 2 \cdot \beta_{k-2} \cdot \alpha_{k-2} \cdot \left(2 \cdot \alpha_{k-2} \cdot (\alpha_{k-3} \pm \eta)^2\right)^3 =$$

$$2^{c(2)} \cdot \beta_{k-2} \cdot \alpha^4_{k-2} \cdot (\alpha_{k-3} \pm \eta)^3$$

$$\frac{\sigma_{k-3}\left(\beta^{(2)}_{k+1}\right)^{2^3}}{\left(\beta^{(2)}_{k+1}\right)^{2^3}} = \frac{\sigma_{k-3}\beta_{k-2} \cdot \sigma_{k-3}\alpha^{2^2}_{k-2}}{\beta_{k-2} \cdot \alpha^{2^2}_{k-2}} = \frac{(-\beta_{k-1}) \cdot \left(\eta^2 \cdot \alpha^{-1}_{k-1}\right)^{2^2}}{\beta_{k-1} \cdot \alpha^{2^2}_{k-1}} = (-1) \cdot \eta^{2^3} \cdot \alpha^{-2^3}_{k-1}$$

Again, by taking 2^3rd root we get

$$\sigma_{k-3}\beta^{(2)}_{k+1} = \zeta^{(2)} \cdot \eta \cdot \beta^{(2)}_{k+1}/\alpha_{k-2},$$

where $\zeta^{(2)}$ is the 2^4th primitive root of unity.
We start by squaring $\beta^{(i)}_{k+1} = \sigma_{k-i}\beta^{(i-1)}_{k+1} + r^{2^{k-d-i}}\beta^{(i-1)}_{k+1}$ thereby using the induction hypothesis according to (a):

$$\sigma_{k-i}\beta^{(i-1)}_{k+1} = \pm r^{2^{k-d-i}} \cdot \eta \cdot \beta^{(i-1)}_{k+1}/\alpha_{k-i+1}$$

$$\left(\beta^{(i)}_{k+1}\right)^2 = \left(\sigma_{k-1}\beta^{(i-1)}_{k+1} + r^{2^{k-d-i}}\beta^{(i-1)}_{k+1}\right)^2 = \left(\beta^{(i-1)}_{k+1}\right)^2 \cdot r^{2^{k-d-i+1}} \cdot \alpha^{-2}_{k-i+1} \cdot (\alpha_{k-i+1} \pm \eta)^2 =$$

$$\left(\beta^{(i-1)}_{k+1}\right)^2 \cdot r^{2^{k-d-i+1}} \cdot \alpha^{-1}_{k-i+1} \cdot 2 \cdot (\alpha_{k-i} \pm \eta).$$

By taking to the power 2^{i-1} this relation becomes:

$$\left(\beta^{(i)}_{k+1}\right)^{2^i} = \left(\beta^{(i-1)}_{k+1}\right)^{2^i} \cdot r^{2^{k-d}} \cdot \alpha^{-2^{i-1}}_{k-i+1} \cdot 2^{2^{i-1}} \cdot (\alpha_{k-i} \pm \eta)^{2^{i-1}}.$$

Now by the induction hypothesis in part (b) we have:

$$\left(\beta^{(i-1)}_{k+1}\right)^{2^i} = 2^{c(i-1)} \cdot \beta_{k-i+1} \cdot \alpha^{2^{i-1}}_{k-i+1} \cdot (\alpha_{k-i} \pm \eta)^{2^{i-1}-1}.$$

$$\left(\beta^{(i)}_{k+1}\right)^{2^i} = 2^{c(i-1)} \cdot \beta_{k-i+1} \cdot \alpha^{2^{i-1}}_{k-i+1} \cdot (\alpha_{k-i} \pm \eta)^{2^{i-1}-1} \cdot (-1) \cdot 2^{2^{i-1}} \cdot \alpha^{-2^{i-1}}_{k-i+1} \cdot (\alpha_{k-i} \pm \eta)^{2^{i-1}} =$$

$$(-1) \cdot 2^{c(i-1)} \cdot 2^{2^{i-1}} \cdot \beta_{k-i+1} \cdot (\alpha_{k-i} \pm \eta)^{2^i-1}.$$

And by squaring for the las time we get:

$$\left(\beta^{(i)}_{k+1}\right)^{2^{i+1}} = 2^{2c(i-1)} \cdot 2^{2^i} \cdot \beta^2_{k-i+1} \cdot \left((\alpha_{k-i} \pm \eta)^2\right)^{2^i-1}.$$

Now by using (12) and (13) and updating the function c by collecting the powers of 2 we get

$$\left(\beta_{k+1}^{(i)}\right)^{2^{i+1}} = 2^{2c(i-1)} \cdot 2^{2^i} \cdot 2 \cdot \beta_{k-i} \cdot \alpha_{k-i} \cdot (2 \cdot \alpha_{k-i} \cdot (\alpha_{k-i-1} \pm \eta))^{2^i-1} =$$

$$2^{2c(i)} \cdot \beta_{k-i} \cdot \alpha_{k-i}^{2^i} \cdot (\alpha_{k-i-1} \pm \eta)^{2^i-1},$$

which completes the proof of (b).

From (10) and (5) we have

$$\frac{\sigma_{k-i-1}\left(\beta_{k+1}^{(i)}\right)^{2^{i+1}}}{\left(\beta_{k+1}^{(i)}\right)^{2^{i+1}}} = (-1) \cdot \eta^{2^{i+1}} \cdot \alpha_{k-i}^{-2^{i+1}}$$

By extracting 2^{i+1}st roots we get

$$\sigma_{k-i-1}\beta_{k+1}^{(i)} = \zeta^{(i)} \cdot \eta \cdot \beta_{k+1}^{(i)}/\alpha_{k-i}, \tag{17}$$

To finish the proof of (a) we have to identify primitive 2^{i+1}st root of unity $\zeta^{(i)}$ up to sign with $r^{k-d-i-1}$. By applying σ to (17) and substituting (17) again we get

$$\sigma_{k-i}\beta_{k+1}^{(i)} = \left(\zeta^{(i)}\right)^2 \cdot \beta_{k+1}^{(i)} \tag{18}$$

On the other hand by definition of $\beta_{k+1}^{(i)}$

$$\sigma_{k-i}\beta_{k+1}^{(i)} = \sigma_{k-i}\left(\sigma_{k-i}\beta_{k+1}^{(i-1)} + r^{2^{k-d-i}}\beta_{k+1}^{(i-1)}\right) = \sigma_{k-i+1}\beta_{k+1}^{(i-1)} + r^{2^{k-d-i}} \cdot \sigma_{k-i}\beta_{k+1}^{(i-1)}$$

By induction hypothesis $\left(\zeta^{(i-1)}\right)^2 = \left(r^{2^{k-d-i}}\right)^2$. Now by using (18) we get

$$\sigma_{k-i}\beta_{k+1}^{(i)} = \left(\zeta^{(i-1)}\right)^2 \cdot \beta_{k+1}^{(i-1)} + r^{2^{k-d-i}} \cdot \sigma_{k-i}\beta_{k+1}^{(i-1)} =$$

$$r^{2^{k-d-i}} \cdot \left(r^{2^{k-d-i}} \cdot \beta_{k+1}^{(i-1)} + \sigma_{k-i}\beta_{k+1}^{(i-1)}\right) = r^{2^{k-d-i}} \cdot \beta_{k+1}^{(i-1)}$$

If we compare this result with (15) we find $\left(\zeta^{(i)}\right)^2 = r^{2^{k-d-i}}$, which leads to the assertion in (a) by taking square roots. The proof of Lemma 1 is complete.

To finish the proof of Theorem 2 we show how (16) is solved by the Lemma 1: If for some $1 \le i \le k-d$ the element $\beta_{k+1}^{(i)}$ is zero then this means by (15) that $\sigma_{k-i}\beta_{k+1}^{(i-1)} = -r^{2^{k-d-i}} \cdot \eta \cdot \beta_{k+1}^{(i-1)}$ - but part (a) of Lemma tells us that $\sigma_{k-i-1}\beta_{k+1}^{(i)} = \pm r^{2^{k-d-i}} \cdot \eta \cdot \beta_{k+1}^{(i)}/\alpha_{k-i}$. So we arrive at $\alpha_{k-i+1} = \pm 1$ which is a contradiction, cause none of the defining elements is contained in base field.

References

[1] Cohen S. D., The explicit construction of irreducible polynomials over finite fields, *Designs, Codes and Cryptography* 2 pp. 169-174, 1992.

[2] Kyuregyan M. K., Recurrent methods for constructing irreducible polynomials over F_q of odd characteristics, *Finite Fields and Their Applications* 9 pp. 39-58, 2003.

[3] Meyn H., Explicit N-Polynomials of 2-Power Degree over Finite Fields, I., *Designs, Codes and Cryptography* 6 pp. 107-116, 1995.

N -բազմանդամների հաջորդականությունների կառուցումը կենտ բնութագրիչներով վերջավոր դաշտերի վրա

Գ. Մ. Համբարձումյան

Ամփոփում

Այս հոդվածում ներկայացված է N-բազմանդամների կառուցման եղանակ $F_q, q \equiv 1 mod(4)$ վերջավոր դաշտերում: Համապատասխան կերպով ընտրված 2 աստիճանի $f_1(x) \in F_q[x]$ N-բազմանդամի համար 2^k աստիճանի $f_1(x) \in F_q[x]$ N-բազմանդամները կառուցվում են $f(x) \to (2x)^{deg(f)} f(\frac{x+\eta^2 x^{-1}}{2}), \eta \in F_q, \eta \neq 0$ ձևափոխության կիրառումով: