Mathematical Problems of Computer Science 31, 16-27, 2008.

Completely Normal Elements in Iterated Quadratic Extensions of Finite Fields of Odd Characteristics

Melsik K. Kyuregyan and Ofelya A. Manukyan

Institute for Informatics and Automation Problems, Armenian National Academy of Sciences
E-mails: melsik@ipia.sci.am, manofa81@yahoo.com

Abstract

In this paper computationally easy explicit constructions of sequences of irreducible and normal monic polynomials over finite fields of odd characteristic are presented.

1. Introduction

We describe possible quadratic transformations over the field F_q, where q is an odd prime power, of the form $P(x) \to (dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right)$ into the ring $F_q[x]$, allowing to construct explicitly irreducible polynomials of higher degree from a suitably chosen irreducible monic polynomial $P(x)=\sum_{i=0}^{n} a_i x^i$ with at least one coefficient $a_{2i+1} \neq 0, (0 \le i \le \left\lfloor \frac{n}{2} \right\rfloor)$.

Proposition 1 ([3], Theorem 2) *Let q be an odd prime power, $P(x) \neq x$ be an irreducible polynomial of degree $n \ge 1$ over F_q, and ax^2+bx+c and dx^2+rx+h be relatively prime polynomials from $F_q[x]$, where $(a,d) \neq (0,0)$ and $r^2 \neq 4dh$. Suppose*

$$(ah)^2+(cd)^2+acr^2+b^2dh-bcdr-abhr-2acdh=\delta^2, \tag{1}$$

for some $\delta \neq 0$ from F_q. Then the polynomial

$$F(x)=(H(a,d))^{-1}(dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right),$$

is irreducible over F_q if and only if the element

$$(r^2-4dh)^n P\left(\frac{br-2(cd+ah-\delta)}{r^2-4dh}\right) P\left(\frac{br-2(cd+ah+\delta)}{r^2-4dh}\right), \tag{2}$$

(denote expression (2) by A) is a non-square in F_q, where

$$H(a,d)=\begin{cases} a^n, \text{if } (d=0) \\ d^n P\left(\frac{a}{d}\right), \text{if } (d \neq 0) \end{cases}.$$

In this paper we investigate $r^2 \neq 4dh$ case. The methods of construction of irreducible polynomials proposed here do not require condition (1) $(ah)^2+(cd)^2+acr^2+b^2dh-bcdr-abhr-2acdh$ to be square in F_q and (A) to be non-square. The new restrictions imposed are: $(r^2-4dh)(b^2-4ac) \neq 0$ and

$hr = 2(cd + ah)$, and $B = (4dh - r^2)^n g\left(\frac{b^2 - 4ac}{4dh - r^2}\right)$ is non-square in F_q, where $g_P(x)$ is the minimal polynomial of the element α^2 in F_q for a root α of the initial polynomial $P(x)$ which, in case of our restrictions on $P(x)$, can be found explicitly (see Proposition 3). There is no restriction on the degree of the initial irreducible polynomial $P(x)$, unlike the methods in [3].

2. Definitions and preliminary results

Let F_q be the Galois field of order $q = p^s$, where p is an odd prime and s is a natural number, with multiplicative group F_q^*. Let, further, $\Gamma(q)$ denote the algebraic closure of F_q. For $P(x) = \sum_{i=0}^{n} a_i x^i \in F_q[x]$ and $\alpha \in \Gamma(q)$, we define $P(x) \circ \alpha = \sum_{i=0}^{n} a_i \alpha^{q^i} = \sum_{i=0}^{n} a_i \sigma^i(\alpha)$, where $\sigma(\alpha) = \alpha^q$ denotes the Frobenius automorphism of F_q. This makes the additive group of $\Gamma(q)$ into a module over $F_q[x]$. For $\alpha \in \Gamma(q)$, we see that $\alpha \in F_{q^m}$ if and only if $(x^m - 1) \circ \alpha = 0$. The additive order of α is defined as the unique monic polynomial $Ord_q(\alpha) \in F_q[x]$, which generates the annihilator of α as an ideal.

An element $\alpha \in \Gamma(q)$ is called *normal* in F_{q^n} over F_q if and only if the set of conjugates $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ constitutes a basis of F_{q^n} as a vector space over F_q. This is exactly the case if $Ord_q(\alpha) = x^n - 1$, which means that the $F_q[x]$-submodule of $\Gamma(q)$ generated by α equals F_{q^n}.

We have an obvious test for an element to have maximal order: $\alpha \in F_{q^n}$ is normal over F_q if and only if $\frac{x^n - 1}{h(x)} \circ \alpha \neq 0$ for all monic irreducible factors $h(x)$ of $x^n - 1$.

If for each factor r of n the conjugates of α over F_{q^r} from F_{q^r}-vector space bases of F_{q^n}, then α is said to be a completely 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 minimal polynomial of an element in a normal basis $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ is $m(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i}) \in F_q[x]$, which is irreducible 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. It is well known that such a basis always exists and any element of N is a generator of N.

We need the following propositions.

Proposition 2 ([5], Theorem 3.7). *Let $P(x) \in F_q[x]$ be an irreducible polynomial of degree n and $f(x)$ and $h(x)$ be relatively prime polynomials from $F_q[x]$. Then $F(x) = h^n(x) P\left(\frac{f(x)}{h(x)}\right)$ is irreducible over F_q if and only if $f(x) - \alpha h(x)$ is irreducible over F_{q^n} for some root $\alpha \in F_{q^n}$ of $P(x)$.*

Define the polynomial $g_P(x)$ *by*

$$g_P(x) = (-1)^n \sum_{j=0}^{n} \sum_{i=0}^{\frac{j}{2}} (-1)^i a_i a_{j-i} x^j ,$$

if $P(x) = \sum_{i=0}^{n} a_i x^i \in F_q[x]$.

Proposition 3 ([3], **Theorem 8**) *Let $P(x) = \sum_{i=0}^{n} a_i x^i \in F_q[x]$ be an irreducible polynomial of degree $n > 1$, with at least one coefficient $a_{2i+1} \neq 0, (0 \le i \le \left\lfloor \frac{n}{2} \right\rfloor)$ and has the order e. Then the polynomial $g_P(x)$ of degree n is irreducible over F_q and has the order $\frac{e}{\gcd(e,2)}$. Moreover, $g_P(x)$ is the minimal polynomial of the element α^2 if α is a root of $P(x)$.*

3. Irreducibility of a composition of polynomials

In this paper we consider only monic polynomials. Let $P(x)$ be an irreducible polynomial of degree n over F_q. Set for $a, d \in F_q$

$$H(a,d) = \begin{cases} a^n, \text{if } (d = 0) \\ d^n P\left(\frac{a}{d}\right), \text{if } (d \neq 0) \end{cases}.$$

Theorem 1. *Let q be an odd prime power and $P(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial of degree $n > 1$ over F_q, with at least one coefficient $a_{2i+1} \neq 0, (0 \le i \le \left\lfloor \frac{n}{2} \right\rfloor)$. Let $ax^2 + bx + c$ and $dx^2 + rx + h$ be relatively prime polynomials from $F_q[x]$, with $(a,d) \neq (0,0)$. Suppose*

$$(r^2 - 4dh)(b^2 - 4ac) \neq 0 \text{ and } br = 2(cd + ah). \tag{3}$$

Then the polynomial

$$F(x) = (H(a,d))^{-1} (dx^2 + rx + h)^n P\left(\frac{ax^2 + bx + c}{dx^2 + rx + h}\right),$$

is monic and irreducible over F_q *if and only if the element B*

$$B = (4dh - r^2)^n g\left(\frac{b^2 - 4ac}{4dh - r^2}\right), \tag{4}$$

is a non-square in F_q.

Proof. Since $P(x)$ is irreducible over F_q, then it can be represented in F_{q^n} as

$$P(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}), \tag{5}$$

for $\alpha \in F_{q^n}$. Substituting $\frac{ax^2 + bx + c}{dx^2 + rx + h}$ for x into (5) and multiplying both sides of the relation by $(dx^2 + rx + h)^n$, we obtain the polynomial $F_1(x)$ as

$$F_1(x)=(dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right)=\prod_{u=0}^{n-1}((a-d\alpha^{q^u})x^2+(b-r\alpha^{q^u})x+(c-h\alpha^{q^u})).$$

By Proposition 2, $F_1(x)$ is irreducible over F_q if and only if the polynomial $(a-d\alpha)x^2+(b-r\alpha)x+(c-h\alpha)$ is irreducible over F_{q^n}. This is equivalent to the condition that the element $D(\alpha)=(r^2-4hd)\alpha^2-2(br-2dc-2ah)\alpha+b^2-4ac$ is a non-square in F_{q^n}. By (3), we obtain

$$D(\alpha)=(4hd-r^2)\left(\frac{b^2-4ac}{4hd-r^2}-\alpha^2\right).$$

The element $D(\alpha)$ is a non-square in F_{q^n} if and only if $(D(\alpha))^{\frac{q^n-1}{2}}=-1$, which is the case if and only if B defined in (4) is a non-square in F_q. Indeed,

$$(D(\alpha))^{\frac{q^n-1}{2}}=\left(\left((4hd-r^2)\left(\frac{b^2-4ac}{4hd-r^2}-\alpha^2\right)\right)^{\frac{q^n-1}{q-1}}\right)^{\frac{q-1}{2}}$$

$$=\left(\prod_{u=0}^{n-1}\left((4hd-r^2)\left(\frac{b^2-4ac}{4hd-r^2}-\alpha^2\right)\right)^{q^u}\right)^{\frac{q-1}{2}}$$

$$=\left(\prod_{u=0}^{n-1}\left(4hd-r^2\right)\left(\frac{b^2-4ac}{4hd-r^2}-\alpha^{2q^u}\right)\right)^{\frac{q-1}{2}}$$

$$=\left((4hd-r^2)^n\left(\frac{b^2-4ac}{4hd-r^2}\right)\right)^{\frac{q-1}{2}}=-1.$$

The penultimate equation holds since, by Proposition 3, $g_P(x)$ is the minimal polynomial of α^2. Observe that since $a-d\alpha$ is a non-zero element in F_{q^n}, we obtain

$$F_1(x)=\prod_{u=0}^{n-1}(a-d\alpha^{q^u})\left(x^2+\left(\frac{b-r\alpha}{a-d\alpha}\right)^{q^u}x+\left(\frac{c-h\alpha}{a-d\alpha}\right)^{q^u}\right)$$

$$=H(a,d)\prod_{u=0}^{n-1}\left(x^2+\left(\frac{b-r\alpha}{a-d\alpha}\right)^{q^u}x+\left(\frac{c-h\alpha}{a-d\alpha}\right)^{q^u}\right)=H(a,d)F(x),$$

where $F(x)=\prod_{u=0}^{n-1}\left(x^2+\left(\frac{b-r\alpha}{a-d\alpha}\right)^{q^u}x+\left(\frac{c-h\alpha}{a-d\alpha}\right)^{q^u}\right)$.

Thus

$$F(x)=H(a,d)^{-1}F_1(x)=H(a,d)^{-1}(dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right),$$

is irreducible over F_q, which completes the proof.

Theorem 1 gives us the following corollary.

Corollary 1. *Let q and the polynomial $P(x)$ satisfy the hypothesis of Theorem 1.*

(1) *if $a,c \in F_q^*$, then the polynomial $F(x) = H(a,0)^{-1}(2ax)^n P\left(\frac{ax^2+c}{2ax}\right)$ is irreducible over F_q if and only if the element $(-1)^n g_P\left(\frac{c}{a}\right)$ is not a square in F_q.*

(2) *if $h,d \in F_q^*$, then the polynomial $F(x) = H(0,d)^{-1}(dx^2+h)^n P\left(\frac{2ax}{dx^2+h}\right)$ is irreducible over F_q if and only if the element $(hd)^n g_P\left(\frac{h}{d}\right)$ is not a square in F_q.*

An element $\alpha \in F_q^n$ is a proper element of F_q^n if $\alpha \notin F_q^v$ for any proper divisor v of n.

Lemma 1. *Let q be an odd prime power and $P(x) \in F_q[x]$ be an irreducible polynomial of degree $n>1$. Let ax^2+bx+c and dx^2+rx+h be relatively prime polynomials from $F_q[x]$ with $(a,d) \neq (0,0)$ and $(b,r) \neq (0,0)$. If the polynomial*

$$F(x) = H(a,d)^{-1}(dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right), \tag{6}$$

is irreducible over F_q, then the polynomial $F(x)$ has at least one non-zero coefficient $a_{2i+1}, (0 \le i < n)$.

Proof. Assume the contrary, namely, that all the coefficients at the terms with odd degree in the polynomial $F(x)$ are equal to zero, i.e. $F(x) = f(x^2)$ for some $f(x) \in F_q[x]$. Since the polynomial $F(x)$ is irreducible then $f(x)$ is also irreducible over F_q. Let α, β and γ be roots of $P(x)$, $F(x)$ and $f(x)$, respectively. Since $P(x)$ and $f(x)$ are irreducible polynomials of degree n over F_q, then $\alpha, \gamma \in F_{q^n}$ and are proper elements of F_{q^n}. Also, since $F(x)$ is an irreducible polynomial of degree $2n$ over F_q, then β is a proper element of $F_{q^{2n}}$. Since β is a zero of $F(x)$, then $\frac{ax^2+bx+c}{dx^2+rx+h}$ is a zero of $P(x)$. Hence by (6) we may assume, without loss of generality, that

$$\frac{a\beta^2+b\beta+c}{d\beta^2+r\beta+h} = \alpha, \tag{7}$$

and, by $F(x) = f(x^2)$ we may assume that $\beta^2 = \gamma$. So, by (7) we obtain $(r\alpha - b)\beta = (a - d\alpha)\gamma + c - h\alpha$. But since b or r are non-zero elements of F_q and α is a proper element in F_{q^n}, then $r\alpha - b \neq 0$. Hence we have $\beta = [(a-d\alpha)\gamma + c - h\alpha]/(r\alpha - b)$ and we may conclude that $\beta \in F_{q^n}$, which is impossible. The lemma is proved.

4. Recurrent methods

Before beginning the study of methods of construction of sequences of irreducible polynomials we set up some notation and preliminary calculations, which we will use for their description throughout the paper.

Let q be an odd prime power and $F_0(x)=\sum_{i=0}^{n}a_i x^{q^i}$ be an irreducible polynomial of degree $n>1$ over F_q, with at least one coefficient $a_{2i+1}\neq 0, (0\le i\le \left\lfloor\frac{n}{2}\right\rfloor)$. Let ax^2+bx+c and dx^2+rx+h be relatively prime polynomials from $F_q[x]$, with $(a,d)\neq(0,0)$ and $(b,r)\neq(0,0)$. Suppose

$$(r^2-4dh)(b^2-4ac)\neq 0 \text{ and } br=2(cd+ah), \tag{8}$$

and the element $A=(4dh-r^2)^n g\left(\frac{b^2-4ac}{4dh-r^2}\right)$ is a non-square in F_q. Then, by Theorem 1, the polynomial

$$\begin{aligned} F_1(x)&=(H(a,d))^{-1}(dx^2+rx+h)^n P\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right)\\ &=(H(a,d))^{-1}(dx^2+rx+h)^n\prod_{u=0}^{n-1}\left(\frac{ax^2+bx+c}{dx^2+rx+h}-\alpha^{q^u}\right), \end{aligned} \tag{9}$$

where α is a root of $F_0(x)$, is irreducible over F_q. Hence by Lemma 1, at least one term of odd degree in the polynomial $F_1(x)$ has a non-zero coefficient. By (9) we have that

$$F_1(-x)=(H(a,d))^{-1}(dx^2-rx+h)^n\prod_{u=0}^{n-1}\left(\frac{ax^2-bx+c}{dx^2-rx+h}-\alpha^{q^u}\right). \tag{10}$$

From expressions (9) and (10) we obtain the relation

$$\begin{aligned} g_1(x^2)&=(-1)^n F_1(x)F_1(-x)=(-1)^n(H(a,d))^{-2}((dx^2+h)^2-r^2x^2)^n\\ &\times\prod_{u=0}^{n-1}\left(\frac{(ax^2+c)^2-b^2x^2}{(dx^2+h)^2-r^2x^2}-\frac{2(adx^2-(ah+cd)x+ch)}{r^2x-(dx+h)^2}-\alpha^{2q^u}\right). \end{aligned} \tag{11}$$

Note that if α_1 is a root of $F_1(x)$, then $g_1(x)$ is the minimal polynomial of α_1^2, (see [3, pp.55-56]), i.e., $g_1(x)=g_{F_1}(x)$.

4.1. Method 1

This method gives an iterative technique for construction of irreducible polynomials over F_q, without imposing any restriction on the degree of the initial irreducible polynomial $F_0(x)$.

Let $a,d,c,h\in F_q^*$. It is easy to see that the equation $adx^2-(cd+ah)x+ch=0$ has non-zero solutions $x_1=ca^{-1}$ and $x_2=hd^{-1}$.

The element $z=\frac{b^2-4ac}{4dh-r^2}$ is non-zero in F_q by (8). Note that the relations

$$z=x_i=\frac{(az+c)^2-b^2z}{r^2z-(dz+h)^2} \quad \text{for } i=1 \text{ or } 2, \tag{12}$$

together with (11) imply

$$g_1(z)=H(0,d)^{-2}((dz+h)^2-r^2z)^n\prod_{u=0}^{n-1}(z-\alpha^{2q^u}),$$

or by Proposition 3

$$g_{F_1}(z)=(H(a,d))^{-2}((dz+h)^2-r^2z)^n g_{F_0}(z). \tag{13}$$

Now let the elements a, b, c, d, r, h satisfy (12). Then we have the following systems of equations:

$$\begin{cases} \dfrac{b^2-4ac}{4dh-r^2}=\dfrac{c}{a} \\ \left(\dfrac{b^2c}{a}-4c^2\right)\left(\left(\dfrac{dc}{a}+h\right)^2-\dfrac{r^2c}{a}\right)=\dfrac{c}{a} \end{cases}, \tag{14}$$

and

$$\begin{cases} \dfrac{b^2-4ac}{4dh-r^2}=\dfrac{h}{d} \\ \left(\dfrac{b^2h}{d}-\left(\dfrac{ah}{d}+c\right)^2\right)\left(4h^2-\dfrac{r^2h}{d}\right)=\dfrac{h}{d} \end{cases}, \tag{15}$$

where the elements a, c, d and h are non-zero, and $(r^2-4dh)(b^2-4ac)\neq 0$ and $br=2(dc+ah)$. The system in (14) has a general solution for

1. $b=2h,\ c=ahd^{-1},\ r=2a$ where $a^2\neq hd$,
2. $b=-2h,\ c=ahd^{-1},\ r=-2a$ where $a^2\neq hd$.

Note that $\dfrac{c}{a}=\dfrac{b^2-4ac}{4dh-r^2}=\dfrac{4h^2-\dfrac{4a^2h}{d}}{4dh-4a^2}=\dfrac{h}{d}$. Therefore, the system (15) has the same general solution.

Hence, for $z=\dfrac{h}{d}$, by (13), we have

$$g_{F_1}\left(\frac{h}{d}\right)=(H_0(a,d))^{-2}\left(\frac{4h}{d}\left(hd-a^2\right)\right)^n g_{F_0}\left(\frac{h}{d}\right). \tag{16}$$

Theorem 2. *Let q and the polynomial $F_0(x)$ satisfy the hypothesis of Theorem 1. Let $ax^2+2hx+ahd^{-1}$ and $dx^2+2ax+h$ be relatively prime, where $a,d,h\in F_q^*$ and $a\neq hd$. Suppose the element $(hd^{-1})^n$ is a non-zero square in F_q and the element $(hd-a^2)^n g_{F_0}\left(\dfrac{h}{d}\right)$ is non-zero square in F_q.* Define

$$F_k(x)=H_{k-1}(a,d)^{-1}(dx^2+rx+h)^n F_{k-1}\left(\frac{ax^2+2hx+ahd^{-1}}{dx^2+2ax+h}\right),$$

for $k\geq 1$, where $H_{k-1}(a,d)=d^{t_{k-1}}F_{k-1}\left(\dfrac{a}{d}\right)$, and t_k is the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over F_q of degree $t_k=n2^k$ for every $k\geq 1$.

Proof. Obviously the degree of $F_k(x)$, $k\geq 0$, is $t_k=n2^k$. Now, let

$$F_k(x)=\sum_{u=0}^{t_k}a_{(k,u)}x^u,\ k\geq 0.$$

We show by induction that the polynomial $F_k(x)$ is irreducible over F_q, for every $k\geq 1$ and has at least one non-zero coefficient $a_{(k,2i+1)}$, $(0\leq i\leq t_k)$. Also, we show that for every $k\geq 1$

$$g_{F_{k+1}}\left(\frac{h}{d}\right)=c_{k-1}^{\ 2}(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right),$$

for some $c_{k-1}\in F_q$.

By assumption $F_0(x)=\sum_{u=0}^{n} a_{(0,u)}x^u$ is irreducible over F_q, with at least one coefficient $a_{(0,2i+1)}\neq 0, (0\le i\le \left\lfloor \frac{n}{2} \right\rfloor)$. Then by Proposition 3, the polynomial $g_{F_0}(x)$ is irreducible over F_q. Since the element $(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right)$ is assumed to be a non-square in F_q, then by Theorem 1, the polynomial

$$F_1(x)=\sum_{u=0}^{t_1} a_{(1,u)}x^u=(H_0(a,d))^{-1}(dx^2+2ax+h)^n F_0\left(\frac{ax^2+2hx+ahd^{-1}}{dx^2+2ax+h}\right),$$

is irreducible over F_q. Moreover, from Lemma 1 follows that the polynomial $F_1(x)$ has at least one non-zero coefficient $a_{(1,2i+1)}\neq 0, (0\le i<n)$. Hence, by Proposition 3, the polynomial $g_{F_1}(x)$ is irreducible over F_q and $g_{F_1}(x)$ is the minimal polynomial of $\alpha_1^{\,2}$ if α_1 is a root of $F_1(x)$. We have the following

$$g_{F_1}\left(\frac{h}{d}\right)=(H_0(a,d))^{-2}\left(\frac{4h}{d}(hd-a^2)\right)^n g_{F_0}\left(\frac{h}{d}\right).$$

Since the element $\left(\frac{h}{d}\right)$ by assumption is a non-zero square in F_q, then

$$g_{F_1}\left(\frac{h}{d}\right)=c_1^{\,2}(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right) \text{ for some } c_1\in F_q.$$

Hence $g_{F_1}\left(\frac{h}{d}\right)$ is a non-square in F_q if $(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right)$ is so.

Next assume that, for some $k\ge 2$, the polynomial $F_{k-1}(x)$ is irreducible over F_q and has at least one non-zero coefficient $a_{(k-1,2i+1)}\neq 0, (0\le i<t_{k-1})$. Also assume that

$$g_{F_{k-1}}\left(\frac{h}{d}\right)=c_{k-1}^{\,2}(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right) \text{ for some } c_{k-1}\in F_q. \tag{17}$$

From the first assumption it follows, by Proposition 3, that the polynomial $g_{F_{k-1}}(x)$ is irreducible over F_q and $g_{F_{k-1}}(x)$ is the minimal polynomial of $\alpha_{k-1}^{\,2}$ if α_{k-1} is a root of $F_{k-1}(x)$. From the second assumption it follows that $g_{F_{k-1}}\left(\frac{h}{d}\right)$ is a non-square in F_q if $(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right)$ is so. Applying Theorem 1, we obtain that $F_k(x)$ is irreducible. Further, by Lemma 1, $F_k(x)$ has at least one non-zero coefficient $a_{(k,2i+1)}\neq 0, (0\le i<t_{k-1})$. Hence, by Proposition 3 the polynomial $g_{F_k}(x)$ is irreducible over F_q and is the minimal polynomial of $\alpha_k^{\,2}$, where α_k is a root of $F_k(x)$. One can show that

$$g_{F_k}\left(\frac{h}{d}\right)=H(a,d)^{-2}\left(\frac{4h}{d}(hd-a^2)\right)^{t_{k-1}} g_{F_{k-1}}\left(\frac{h}{d}\right).$$

Using (17), we obtain $g_{F_k}\left(\frac{h}{d}\right)=c_k^{\,2}(hd-a^2)^n g_{F_0}\left(\frac{h}{d}\right)$ for some $c_k\in F_q$, which completes the proof.

4.2. Method 2

Let $d=0$ and $a,c\in F_q^*$ and $b,r,h\in F_q$. In this case, by (8), we have $r(b^2-4ac)\neq 0$ and $br-2ah$. Then the element $z=-\dfrac{b^2-4ac}{r^2}$ is non-zero. If for the element the relations $\dfrac{b^2z-(az+c)^2}{h^2-r^2z}=z$ and $ahz=ch$ hold, then from (11) we have

$g_{F_1}(z)=(H(a,0))^{-2}(h^2-r^2z)^n\prod_{s=0}^{n-1}(z-\alpha^{2s})$ or by Proposition 3

$$g_{F_1}(z)=(H(a,0))^{-2}(h^2-r^2z)^n g_{F_0}(z). \tag{18}$$

Now, let the elements a, b, c, h and r be the solutions of the following system of equations:

$$\begin{cases} br=2ah \\ \dfrac{b^2z-(az+c)^2}{h^2-r^2z}=z \\ ahz=ch \end{cases},$$

where the elements a, c, r are non-zero, and $b^2\neq 4ac$ and $z=-\dfrac{b^2-4ac}{r^2}$. It is easy to see that this system has a non-zero solution only for

$$b=h=0;\ r=\pm 2a;\ a,c\in F_q^*. \tag{19}$$

In case of (19) $z=\dfrac{c}{a}$, and by (18) we have $g_{F_1}\left(\dfrac{c}{a}\right)=(H(a,0))^{-2}(-4ac)^n g_{F_0}\left(\dfrac{c}{a}\right)$.

Using these preliminary computations, one can prove the following theorem in a manner similar to Theorem 2.

Theorem 3. *Let q and the polynomial $F_0(x)$ satisfy the hypothesis of Theorem 1. Suppose $a,c\in F_q^*$ and $(ac)^n$ is a square in F_q and the element $(-1)^n g_{F_0}\left(\dfrac{c}{a}\right)$ is a non-square in F_q.* Define

$$F_k(x)=(2x)^{t_{k-1}}F_{k-1}\left(\frac{ax^2+c}{2ax}\right), k\geq 1,$$

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

In particular, when $q\equiv 3(\mathrm{mod}\,4)$, $F_0(x)=x^2+2x+c$ and $a=1$, Theorem 3 is in agreement with McNay's theorem in [4]. Theorem 3 as Theorem 6 from [3], gives a recurrent method for constructing irreducible polynomials of degree $n2^k$, for arbitrary integers $n,k\geq 1$, over any field of odd characteristic.

The case $a=c=1$ of Theorem 3 was proved by Cohen in [2] under the additional assumption that n is even when $q\equiv 3(\mathrm{mod}\,4)$.

In the following theorem we construct completely normal elements in F_q, $q\equiv 1(\mathrm{mod}\,4)$. In the proof we use Chapman's method to prove the normality and complete normality of elements in F_{q^n} over F_q, see [1].

Theorem 4. *Let $q \equiv 1 \pmod 4$ be a prime power, and $F_1(x) = x^2 + bx + c$ be a quadratic polynomial over F_q, where b is non-zero, and c is a non-zero square and $b^2 - 4c$ is a non-square in F_q. Define $F_k(x), k \geq 2$, recursively by*

$$F_k(x) = (2x)^{t_{k-1}} F_{k-1}\left(\frac{x^2 + c}{2x}\right).$$

Then $F_k(x), k \geq 1$, is an N-polynomial of degree $t_k = 2^k$ over F_q. Further, if α_k is a zero of $F_k(x)$, then α_k is a completely normal element of $F_{q^{t_k}}$ over F_q, $k \geq 2$.

Proof. First note that $F_1(x) = x^2 + bx + c$ is irreducible over F_q since $b^2 - 4c$ *is a non-square in* F_q. Then by Proposition 3 $g_{F_1}(x) = x^2 + (2c - b^2)x + c^2$ and $(-1)^2 g_{F_1}(c) = c(4c - b^2)$. Hence $g_{F_1}(c)$ is a non-square in F_q because c is a non-zero square in F_q and $4c - b^2$ is non-square in F_q. Therefore, according to Theorem 3, the polynomial $F_k(x), k \geq 2$, is irreducible over F_q.

Our first task is to show that α_k is a normal element of $F_{q^{t_k}}$ over F_q. If α is a zero of polynomial $F_k(x)$ then $\frac{\alpha^2 + c}{2\alpha}$ is a zero of $F_{k-1}(x)$, so we may assume that $\alpha_{k-1} = \frac{\alpha_k^2 + c}{2\alpha_k}$ for all $k \geq 2$. Now let $\gamma_k = \frac{\alpha_k + \sqrt{c}}{\alpha_k - \sqrt{c}}$ for $k \geq 1$, where by the term $\sqrt{c}$ we mean a fixed square root of c inside F_q. Then

$$\gamma_k^2 = \frac{\alpha_k^2 + 2\sqrt{c}\alpha_k + c}{\alpha_k^2 - 2\sqrt{c}\alpha_k + c} = \frac{2\alpha_k\alpha_{k-1} + 2\sqrt{c}\alpha_k}{2\alpha_k\alpha_{k-1} - 2\sqrt{c}\alpha_k} = \gamma_{k-1}.$$

Also, let $\gamma_0 = \gamma_1^2 = \frac{\alpha_1^2 + 2\sqrt{c}\alpha_1 + c}{\alpha_1^2 - 2\sqrt{c}\alpha_1 + c} = \frac{-b\alpha_1 + 2\sqrt{c}\alpha_1}{-b\alpha_1 - 2\sqrt{c}\alpha_1} = \frac{-b + 2\sqrt{c}}{-b - 2\sqrt{c}} \in F_q$. Note that $\alpha_k = \frac{\sqrt{c}(\gamma_k + 1)}{(\gamma_k - 1)}$. Consider $\beta_k = \alpha_k - \alpha_{k-1}$ for $k \geq 2$.

We have $\beta_k = \frac{\sqrt{c}(\gamma_k + 1)}{\gamma_k - 1} - \frac{\sqrt{c}(\gamma_k^2 + 1)}{\gamma_k^2 - 1} = \frac{2\sqrt{c}\gamma_k}{\gamma_k^2 - 1}$.

We show by induction on k that $Ord_q(\alpha_k) = x^{2^k} - 1$. If $k = 1$, then $\alpha_1 \notin F_q$. therefore, $(x-1) \circ \alpha_1 \neq 0$ and $(x+1) \circ \alpha_1 = -a \neq 0$. It follows that $Ord_q(\alpha_1) = x^2 - 1$ as required. Now let $k > 1$. By the inductive hypothesis we may assume that $Ord_q(\alpha_{k-1}) = x^{2^{k-1}} - 1$. It will suffice to show that $Ord_q(\beta_k) = x^{2^{k-1}} + 1$, since $x^{2^{k-1}} - 1$ and $x^{2^{k-1}} + 1$ are coprime and $\alpha_k = \alpha_{k-1} + \beta_k$. We need the factorization of $x^{2^{k-1}} + 1$ over F_q.

4.3. Method 3

Let $a = 0$, $d, h \in F_q^*$ and $c, b, r \in F_q$. In this case, by (8), we have $b(r^2 - 4dh) \neq 0$ and $br = 2dc$. Then the element $z = \frac{b^2}{4dh - r^2}$ is non-zero.

If for the element z the relations $\frac{b^2z-c^2}{(dz+h)^2-r^2z}=z$ and $cdz=ch$ hold, then from (11) we have

$$g_1(z)=H(0,d)^{-1}((dz+h)^2-r^2z)^n\prod_{u=0}^{q-1}(z-a^{2u}). \tag{20}$$

Let the element b, c, d, h and r be solutions of the following system of equations:

$$\begin{cases} br=2dc \\ \dfrac{b^2z-c^2}{(dz+h)^2-r^2z}=z \\ cdz=ch \end{cases},$$

where the elements b, d and h are non-zero and $r^2\neq 4dh$ and $z=\dfrac{b^2}{4dh-r^2}$. It is easy to see that this system has a non-zero solution only for $c=r=0$, $b=\pm 2h$, $d,h\in F_q^*$. Hence, $z=\dfrac{h}{d}$, and by (20) we have

$$g_{t_k}\left(\frac{h}{d}\right)=(H(0,d))^{-2}(4h^2)^n g_{t_k}\left(\frac{h}{d}\right).$$

Using these preliminary computations, one can prove the following theorem in a manner similar to Theorem 2.

Theorem 5. *Let q and the polynomial $F_0(x)$ satisfy the hypothesis of Theorem 1. Suppose $h,d\in F_q^*$ and $(dh)^n$ is a square in F_q, and the element $g_{t_k}\left(\dfrac{h}{d}\right)$ is a non-square in F_q.* Define

$$F_k(x)=H_{k-1}(0,d)^{-1}(dx^2+h)^{t_{k-1}}F_{k-1}\left(\frac{2hx}{dx^2+h}\right), k\geq 1,$$

where $H_{k-1}(0,d)=d^{t_{k-1}}F_{k-1}(0)$ and t_k denotes the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over F_q of degree $t_k=n2^k$ for every $k\geq 1$.

For $d=h=1$, Theorem 5 gives the following corollary.

Corollary 2. *Let q and the polynomial $F_0(x)$ satisfy the hypothesis of Theorem 1. Suppose the element $g_{t_k}(1)$ is a non-square in F_q.* Define

$$\begin{cases} F_1(x)=(F_0(0))^{-1}(x^2+1)^n F_0\left(\dfrac{2x}{x^2+1}\right) \\ F_k(x)=(x^2+1)^{t_{k-1}}F_{k-1}\left(\dfrac{2x}{x^2+1}\right), k\geq 2 \end{cases}, \tag{21}$$

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

The sequence of functions (21), constructed in the above corollary, is shown to be irreducible in [3] under the restrictions: $F_0(1)F_0(-1)$ is a non-square in F_q and the degree of the initial polynomial $F_0(x)$ is even if $q\equiv 3(\mathrm{mod}\,4)$.

References

[1] R. Chapman, "Completely normal elements in iterated quadratic extensions of finite fields", *Finite Fields Appl.*, Volume 3, pp. 3-10, 1997.

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

[3] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over F_q of odd characteristics", *Finite Fields Appl.*, Volume 9, pp. 39-58, 2003.

[4] G. McNay, Topics in finite fields, *Ph.D. Thesis, University of Glasgow*, 1995.

[5] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, "Applications of Finite Fields", *Kluwer Publishers, Boston, Dordrecht, Lancaster*, 1993.

[6] H. Meyn, "Explicit N-polynomials of 2-power degree over finite fields", I, *Designs, Codes and Cryptography*, Volume 6, pp. 107-116, 1995.

Կենտ բնութագրիչով վերջավոր դաշտերի քառակուսային իռներատիվ ընդլայնումների վրա ամբողջական նորմալ տարրեր

Մ. Կյուրեղյան և Օ. Մանուկյան

Ամփոփում

Ներկայացված են չբերվող և նորմալ բազմանդամների հաջորդականությունների կառուցման ալգորիթմներ, որոնք հաշվողական տեսանկյունից հեշտ են և տալիս են բազմանդամների բացահայտ տեսքերը: