Construction of Irreducible Polynomials with Given Orders

Melsik K. Kyureghyan
Institute for Informatics and Automation Problems of NAS RA
e-mail: melsik@ipia.sci.am

Sergey Abrahamyan
Institute for Informatics and Automation Problems of NAS RA
e-mail: serj.abrahamyan@gmail.com

Knarik M. Kyuregyan
Institute for Informatics and Automation Problems of NAS RA
e-mail: knarikyuregyan@gmail.com

ABSTRACT
In this paper we propose an effective method for constructing irreducible polynomials over finite fields with given orders.

Keywords
Galois field, Irreducible polynomial, Order.

1. INTRODUCTION
It is well known that sequences (maximal length sequences) over finite fields receive numerous applications in various disciplines including in the design of stream ciphers. For all practical purposes these sequences are generally considered over binary fields. The sequences with maximal period have been proved to have good cryptographic properties. Construction of large sequences are equivalent to the construction of irreducible polynomials with large order over finite field. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial of degree n over F_2 belonging to order e. In this paper an effective implementation of irreducible polynomials construction method is presented proposed by M. Kyureghyan and G. Kyureghyan in [3]. Denote that there is an impressive amount of papers devoted to the construction of high degree irreducible polynomials, however only a few of them consider the order of constructed irreducible polynomials [2].

The organization of the paper is as follows: in section 2 we introduce some preliminary results. In section 3 we present a new method for constructing irreducible polynomials with given orders.

2. PRELIMINARIES
Let F_q be the Galois field of order $q = p^s$, where p is an odd prime and s is a natural number.

Proposition 1 ([1], Theorem 3.46) Let $f(x)$ be a monic irreducible polynomial of degree n over F_q and let $k \in N$. Then $f(x)$ factors into d irreducible polynomials in $F_{q^k}[x]$ of the same degree n/d, where $d = \gcd(n, k)$.

Next proposition is an immediate consequence of Proposition 1.

Proposition 2 ([1], Corollary 3.47) An irreducible polynomial over F_q of degree n remains irreducible over F_{q^k} if and only if n and k are relatively prime.

Moreover if $g(x) = \sum_{i=0}^{n/d} g_i x^i \in F_{q^d}[x]$ is a factor of $f(x)$ then the remaining factors are

$$g^{(u)}(x) = \sum_{i=0}^{n/d} g_i^{q^u} x^i.$$

In [3] the authors have proposed a new method for constructing higher degree irreducible polynomials over finite field F_q.

Proposition 3 ([3], Theorem 1) Let $n > 1$, $\gcd(n, k) = 1$ and $f(x)$ be an irreducible polynomial of degree n over F_q. Further let $\alpha \neq 0$ and β be elements of F_{q^k}. Set $g(x) = f(\alpha x + \beta)$. Then the polynomial

$$F(x) = \prod_{a=0}^{k-1} g^{(a)}(x)$$

of degree nk is irreducible over F_q if and only if $F_q(\alpha, \beta) = F_{q^k}$.

Recall that besides the degree there is another important integer attached to a nonzero polynomial over a finite field namely its order.

Proposition 4 Let $g_1, g_2 \in F_q^*$, g_1 belonging to order e_1, g_2 belonging to order e_2 and $gcd(e_1, e_2) = 1$. Then $g_1 g_2$ belonging to order $e_1 e_2$.

3. CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS WITH GIVEN ORDERS
The paper is devoted to the effective implementation of Proposition 3. This implementation method allows to construct higher degree irreducible polynomials with the necessary order from the given irreducible polynomials with known orders.

Let $gcd(n, m) = 1$, $f(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial of degree $n > 1$ over F_2 belonging to order e, and let α be a root of irreducible polynomial $g(x) \in F_2[x]$ of degree m belonging to order t. Based on Proposition 3 we show that the polynomial

$$F(x) = \prod_{u=0}^{m-1} \left(\sum_{i=0}^{t-1} \left(\sum_{j=0}^{k} a_{jt+i} x^{jt+i} \right) \alpha^{(2^u i) mod t} \right) \quad (1)$$

is an irreducible polynomial of degree nm over F_2 belonging to oreder et.

By Proposition 2 the polynomial $f(x) \in F_2[x]$ of degree n will be irreducible over F_{2^m} also. Denote $g^{(i)}(x) := f\left(\alpha^{2^i} x\right)$, where $i = 0, 1, 2, \ldots, m-1$. By Proposition

3 the polynomial

$$F(x)=\prod_{u=0}^{m-1} g^{(u)}(x) \tag{2}$$

is an irreducible polynomial of degree nm over F_2.

Next we get the explicit view of the polynomial $g^{(u)}(x)$ for $u=0,1,\dots,m-1$.

Let's take the number k such that $kt\le n$. Then for $u=0,1,\dots,m-1$

$$g^{(u)}(x)=f\left(\alpha^{2^u}x\right)=\left(a_0+a_t x^t+\cdots+a_{kt}x^{kt}\right)$$

$$+(a_1x+a_{t+1}x^{t+1}+\cdots+a_{kt+1}x^{kt+1})\alpha^{2^u modt}$$

$$+\left(a_2x^2+a_{t+2}x^{t+2}+\cdots+a_{kt+2}x^{kt+2}\right)\alpha^{(2\cdot 2^u)modt}+\cdots$$

$$+(a_{t-1}x^{t-1}+a_{2t-1}x^{2t-1}+\cdots+a_{(k+1)t-1}x^{(k+1)t-1})$$

$$\times\alpha^{((t-1)\cdot 2^u)modt}. \tag{3}$$

If we denote

$$f_i(x):=\sum_{j=0}^{k} a_{jt+i}x^{jt+i},\ for\ i=0,1,\dots,t-1,$$

then from (3) we will have

$$g^{(u)}(x)=\sum_{i=0}^{n} a_i\alpha^{2^u i}x^i=\sum_{i=0}^{t-1} f_i\alpha^{(2^u i)modt},$$

where $u=0,1,\dots,m-1$. Substituting $g^u(x)$ in the (2) irreducible polynomial we obtain

$$F(x)=\prod_{u=0}^{m-1}\left(\sum_{i=0}^{t-1} f_i\alpha^{(2^u i)modt}\right).$$

Now let us compute the order of $F(x)$. Let γ be a zero of $f(x)$, then $\alpha^{-1}\gamma$ will be the root of the polynomial $f(\alpha x)$. Therefore it is enough to compute the order of $\alpha^{-1}\gamma$. Taking into account that $gcd(n,m)=1$ we have $gcd(2^n-1;2^m-1)=1$ [1]. On the other hand as $\alpha\in F_{2^m}$ and $ord(\alpha)=t$ hence $t|2^m-1$, similarly $\gamma\in F_{2^n}$ and $ord(\gamma)=e$ hence $e|2^n-1$, so one can concludes that $gcd(e,t)=1$. Hence by Proposition 4 the order of $F(x)$ will be equal to et.

Proposed implementation method gives us an opportunity to avoid the operations over extended field. Below the provided examples are particular cases for this implementation.

Example 1 $f(x)=\sum_{i=0}^{n} a_i x^i\in F_2[x]$ is an irreducible polynomial belonging to order e,$g(x)=x^2+x+1\in F_2[x]$ is an irreducible polynomial of order 3 and $g(\alpha)=0$. Hence from (1)

$$F(x)=\left(f_0+f_1\alpha+f_2\alpha^2\right)\cdot(f_0+f_1\alpha^2+f_2\alpha),$$

where

$$f_i(x)=\sum_{j=0}^{k} a_{3j+i}x^{3j+i},\ \ i=0,1,2,\ 3k\le n. \tag{4}$$

Considering that $\alpha^2+\alpha+1=0$ we obtain

$$F(x)=f_0^2+f_1^2+f_2^2+f_0f_1+f_0f_2+f_1f_2. \tag{5}$$

[1]It is well known fact that $gcd(2^a-1,2^b-1)=2^{gcd(a,b)}-1$ for non-negative a and b.

Let $f(x)=x^5+x^2+1\in F_2[x]$ belonging to order 31: $e=31$. From (4) we will have $f_0(x)=1$, $f_1(x)=0$, $f_2(x)=x^5+x^2$ and from (5)

$$F(x)=1+\left(x^5+x^2\right)^2+\left(x^5+x^2\right)=x^{10}+x^5+x^4+x^2+1.$$

Thus we have constructed an irreducible polynomial of degree 10 belonging to order 93:

$$F(x)=x^{10}+x^5+x^4+x^2+1.$$

Example 2 $f(x)=\sum_{i=0}^{n} a_i x^i\in F_2[x]$, $ord(f)=e$ and $g(x)=x^3+x+1\in F_2[x]$, $ord(g)=7$, $g(\alpha)=0$. Hence from (1)

$$F(x)=\left(f_0+f_1\alpha+f_2\alpha^2+f_3\alpha^3+f_4\alpha^4+f_5\alpha^5+f_6\alpha^6\right)$$

$$\times\left(f_0+f_1\alpha^2+f_2\alpha^4+f_3\alpha^6+f_4\alpha+f_5\alpha^3+f_6\alpha^5\right)$$

$$\times\left(f_0+f_1\alpha^3+f_2\alpha^6+f_3\alpha^2+f_4\alpha^5+f_5\alpha+f_6\alpha^4\right),$$

where

$$f_i(x)=\sum_{j=0}^{k} a_{7j+i}x^{7j+i},\ \ i=0,1,2,\dots,6,\ 7k\le n. \tag{6}$$

Considering that $\alpha^4+\alpha^2+\alpha=0$ and $\alpha^6+\alpha^5+\alpha^3=1$ we will have

$$F(x)=f_0^3+f_1^3+f_2^3+f_3^3+f_4^3+f_5^3+f_6^3+f_0^2f_3+f_0^2f_5+f_0^2f_6$$

$$+f_1^2f_0+f_1^2f_4+f_1^2f_6+f_2^2f_0+f_2^2f_1+f_2^2f_5+f_3^2f_1+f_3^2f_2$$

$$+f_3^2f_6+f_4^2f_0+f_4^2f_2+f_4^2f_3+f_5^2f_1+f_5^2f_3+f_5^2f_4+f_6^2f_2$$

$$+f_6^2f_4+f_6^2f_5+f_0f_1f_2+f_0f_1f_4+f_0f_1f_5+f_0f_1f_6+f_0f_2f_3$$

$$+f_0f_2f_4+f_0f_2f_5+f_0f_3f_4+f_0f_3f_5+f_0f_3f_6+f_0f_4f_6$$

$$+f_0f_5f_6+f_1f_2f_3+f_1f_2f_5+f_1f_2f_6+f_1f_3f_4+f_1f_3f_5$$

$$+f_1f_3f_6+f_1f_4f_5+f_1f_4f_6+f_2f_3f_4+f_2f_3f_6+f_2f_4f_5$$

$$+f_2f_4f_6+f_2f_5f_6+f_3f_4f_5+f_3f_5f_6+f_4f_5f_6. \tag{7}$$

Let $f(x)=x^4+x^3+1$ belonging to order 15, then from (6) we get $f_0(x)=1$, $f_3(x)=x^3$, $f_4(x)=x^4$, $f_i(x)=0$ for $i=1,2,5,6$. Hence from (7)

$$F(x)=x^{12}+x^{11}+x^9+x^8+x^7+x^3+1$$

and $ord(F)=7\cdot 15=105$.

So in these examples we have shown how to construct irreducible polynomials of order 93 and 105.

REFERENCES

[1] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, 1987.

[2] M.Kyuregyan, Recurent Methods for constructing irreducible polynomials over F_q of odd characteristics, Finite Fields Applic. 9 (2003) 39-58.

[3] M. Kyureghyan, G.Kyureghyan. "Irreducible Compositions of Polynomials over Finite Fields", Design Codes and Cryptography 61(3), 301–314, 2011.