ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ

ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ

ԻՆՍՏԻՏՈՒՏ

ՍԱԻԴ ՄԵՀՐԱԲԻ

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՎՐԱ ԱՆՎԵՐԱԾԵԼԻ ԵՎ ՆՈՐՄԱԼ ԲԱԶՄԱՆԴԱՄՆԵՐԻ ՌԵԿՈՒՐՍԻՎ ԿԱՌՈՒՑՈՒՄՆԵՐ

Ե.13.05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ ֆիզիկամաթեմատիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան 2013

INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS OF NAS RA

SAEID MEHRABI

RECURSIVE CONSTRUCTIONS OF IRREDUCIBLE AND NORMAL POLYNOMIALS OVER FINITE FIELDS

A U T H O R ' S A B S T R A C T

For obtaining candidate degree in Physical-mathematical sciences in specialty 05.13.05 "Mathematical modeling, numerical methods and software complexes"

Yerevan 2013

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝ ֆիզ. մաթ. գիտ. թեկնածու Մ.Կ.Կյուրեղյան

Պաշտոնական ընդիմախոսներ՝ տեխ. գիտ. դոկտոր Գ.Հ.Խաչատրյան

ֆիզ. մաթ. գիտ. թեկնածու Ժ.Գ.Մարգարյան

Առաջատար կազմակերպություն՝ Երևանի պետական համալսարան

Պաշտպանությունը կայանալու է 2013թ. Հոկտեմբերի 2–ին ժ. 16:00-ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում (հասցեն՝ 0014, Երևան, Պ. Սևակի փ. 1)

Ատենախոսությանը կարելի է ծանոթանալ ԻԱՊԻ-ի գրադարանում:

Սեղմագիրն առաքվել է 2013թ. Սեպտեմբերի 2-ին:
Մասնագիտական խորհուրդի գիտական քարտուղար
ֆիզ. մաթ. գիտ. դոկտոր Հ. Գ. Սարուխանյան

The subject of the dissertation has been approved in the Institute for Informatics and Automation Problems of NAS RA.

Scientific advisor: Cand. of Phys. and Math. Sci. M. K. Kyureghyan

Official opponents: Doctor of Tech. Sci. G.H.Khachatryan

Cand. Of Phys. and Math. Sci. J.G.Margaryan

Leading organization: Yerevan State University

The defense will take place on 2 October, 2013 at 16:00 in the Institute for Informatics and Automation Problems of NAS RA, during the session of the Special Council 037 “Informatics and computer systems” (address: 1P. Sevak Str. 0014, Yerevan)

The dissertation is available at the library of institute.
Author’s abstract is sent on 2 September, 2013.

Scientific secretary of the specialized council,

Doctor of Phys. and Math. Sciences H. G. Sarukhanyan

CHARACTERIZATION OF THE THESIS

The Actuality of the Problem

The theory of finite fields is a branch of modern algebra that the origins of finite fields are from the 17th and 18th centuries. The theory of finite fields as we know it today was constructed at the end of the 18th century and during the 18th century. The next big step in the construction of finite fields was provided by Richard Dedekind on 1857. He characterized the finite fields of order p^n as residue class rings $F_p[x]/f$, where f is an irreducible polynomial of degree n over F_p. Also he introduced the Mobius inversion formula in finite fields to study the number of irreducible polynomials of certain degree. Finally, Eliakim H. Moore in 1893 proved that finite fields must have p^n elements, where p is a prime. By the end of the 19th century all the structure of finite fields was known. Dickson's book (1901) already has all the important elements of this structure. This thesis deals with the explicit methods for finding irreducible polynomials and N-polynomials over finite fields that are important problems in finite fields.

For a prime power q and an integer $n > 1$, let F_q be a finite field with q elements, and F_{q^n} be its extension of degree$n$. Extensions of finite fields are important in implementing cryptosystems and error correcting codes. One way of constructing extensions of finite fields is via an irreducible polynomial over the ground field with degree equal to the degree of the extension. Therefore, finding irreducible polynomials and testing the irreducibility of polynomials are fundamental problems in finite fields. There are two methods for constructing irreducible polynomials over finite fields. The first method is testing method that is based on this theorem.

Theorem 1. For every finite field F_q and every $n \in N$, the product of all monic irreducible polynomials whose degree divides n is equal to$x^{q^n} - x$.

The well-known testing algorithm are due to Ben-Or (1981) and Rabin (1980). The references for these works can be found in von zur Gathen and Panario (2001).

The second method is polynomial composition method that allows constructions of irreducible polynomials of higher degree from given irreducible polynomials over finite fields. This method has been studied by Varshamov, Cohen, Kyuregyan and others.

Another problem that is important for us in this thesis is finding normal element in F_{q^n}, on the other hand an N-polynomial overF_q. An element $\alpha \in F_{q^n}$ is called normal if

$$\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$$

is a basis of F_{q^n} over F_q. In this case, the basis is called a normal basis. For any prime power q and positive integer$n$, there is a normal basis for F_{q^n} over F_q (Eisenstein (1850), Schonemann (1850) and Hensel (1888)). Also the number of normal elements in F_{q^n} over F_q was determined by (Ore 1934). To construct a normal element inF_{q^n}, one simple method is to draw an element at random uniformly fromF_{q^n}, test if it is normal, and repeat until a normal element is obtained (Hensel 1888, von zur Gathen & Giesbrecht 1990). By polynomial composition method in an explicit method way also we can find N-polynomials over finite fields. How to methodologically generate higher degree or efficient normal bases in extension field has been studied for a long time. It is an important and theoretically interesting problem for researchers because, different from polynomial basis, every set of conjugate elements does not form a normal basis. Moreover, some cryptographic schemes efficiently use normal basis by which the calculation costs of some cryptographic operations are substantially reduced. In a normal basis representation, squaring can be performed simply by a cycle shift of the coordinates of an element and, hence, in hardware, it is almost free of cost. Such a cost advantage often makes the normal basis a preferred choice of representation. The first time Massey and Omura proposed a normal basis multiplication scheme which can be implemented in bit-parallel fashion using n identical logic blocks whose inputs are cyclically shifted from one another.

The Objective and the Problems of the Thesis

The main aims of the present investigation are:

1. Finding new recurrent methods for constructing families of irreducible polynomials and N-polynomials over finite fields

2. Factorization of some composite polynomials and finding their irreducible factors,

3. Compute of complexity some N-polynomials over finite fields.

Objects of Investigations

In this thesis, some recurrent methods for constructing families of irreducible polynomials and N-polynomials over finite fields are studied.

Methods of Investigations

In the work, we apply methods of finite fields theory, linear algebra, number theory and programming by using Mat lab software.

The Practical and Theoretical Significance of the Results

The results of the thesis can be used in different applications of coding theory and cryptography.

Publications

The results of the thesis are presented in 7 scientific articles; the list of them is listed at the end of the text.

The Structure and Volume of the Work

The dissertation consists of Introduction, three Chapters, Conclusion and some programs in Appendix A for computing complexity of N-polynomials and factorization some polynomial compositions. The list of references includes 121 entries. The text of the thesis is expounded on 100 pages.

Brief Contents of the Work

In Introduction, the necessary definitions of Finite Fields, e.g. irreducible polynomials, N-polynomials, trace and norm function, testing and explicit methods also in section of outline of thesis the aims and the problems of the dissertation are formulated. In Chapter 2 as main part of this thesis we introduce some constructions of irreducible polynomials and N-polynomials over finite fields. In addition by using some transformations we reach to this aim. We mention summary of results obtained in this chapter. In Part 2.1, we introduce Q-transformation. Varshamov proved that this transformation can be used to produce an infinite sequence of irreducible polynomials over F_2. Kyuregyan suggested a more general construction over F_{2^s}. In this part we show that this transformation can construct families of irreducible polynomials over F_{3^s}. Our result is stated as follows:

Theorem 2. Let $F_1(x)$ be an irreducible polynomial of degree n over F_{3^s}, and n is even when $q \equiv 3 \ (mod\ 4)$. Then

$$F_{k+1}(x) = x^{n2^{k-1}} F_k(x + \delta^2 x^{-1}), \ \ k \geq 1,$$

is an irreducible polynomial of degree $n2^k$ over F_{3^s} if and only if

$$g_{F_1}(\delta^2) = (-1)^n F_1(-\delta) F_1(\delta),$$

be non-square in F_{3^s}.

We present the proof of the theorem in Section 2.1 of Chapter 2. Also we show this transformation can construct families of N-polynomials over F_{3^s} as follows:

Theorem 3. Let $q = 3^s$ where s is even number ($q \equiv 1\ (mod\ 4)$) and $F_1(x) = x^2 + bx + \delta^2$ a quadratic polynomial over F_{3^s} where b, δ are non-zero and $b^2 - \delta^2$ is a non-square in F_{3^s}. Define $F_k(x),\ k \geq 2$ recursively by

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

Then the sequence $F_k(x), k \geq 1$ is a trace-compatible sequence of N-polynomials of degree $t_k = 2^k$ over F_{3^s}. Further if α_k is a zero of $F_k(x)$ then α_k is a completely normal element of $F_{3^{s2^k}}$ over F_{3^s} for$k \geq 2$.

We present the proof of the theorem in Section 2.1 of Chapter 2.

Theorem 4. Let $q = 3^s$ where s is odd number ($q \equiv 3\ (mod\ 4)$) and $F_1(x) = x^2 + bx + \delta$ is a quadratic polynomial over F_{3^s} where b is non-zero and $b^2 - \delta$, are non-square in F_{3^s}. Define $F_k(x),\ k \geq 2$, recursively by

$$F_k(x) = x^{t_{k-1}} F_{k-1}(x + \delta x^{-1}),\ \ k \geq 1.$$

Then the sequence $F_k(x), k \geq 1$ is a trace-compatible sequence of N-polynomials of degree $t_k = 2^k$ over F_{3^s}. Further if α_k is a zero of $F_k(x)$ then α_k is a completely normal element of $F_{3^{s2^k}}$ over F_{3^s} for $k \geq 2$.

We present the proof of the theorem in Section 2.1 of Chapter 2. In Part 2.2 we use the transformation $\rightarrow \frac{x^p - x + \delta_0}{x^p - x + \delta_1}$. F_p fields are proposed for cryptographic purposes where p is relatively small. In particular, some authors describe an implementation of ECDSA over fields of characteristic 3 and 7. Some researchers describe a method to implement elliptic curve cryptosystems over fields of small odd characteristic.

By using this transformation we obtain the following theorem:

Theorem 5. Let $P(x) = \sum_{i=0}^{n} c_i x^i$, with $P(x) \neq x$ be an irreducible polynomial of degree n over F_q, and let its reciprocal $P^*(x)$ be an N-polynomial over F_q. Set

$$F(x) = (x^p - x + \delta)^n P\left(\frac{x^p - x}{x^p - x + \delta}\right),$$

Where $\delta \in F^*_q$. Then $F^*(x)$ is an N-polynomial of degree np over F_q if and only if

$$\left(n + \frac{c_1}{c_0}\right) Tr_{q|p}(\delta \frac{\acute{P}(1)}{P(1)} - n\delta) \neq 0.$$

We present the proof of the theorem in Section 2.2 of Chapter 2.

Based on above theorem a recurrent method for constructing families of N-polynomials of degree np^k over F_q is stated.

Theorem 6. Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over F_q and $P^*(x)$ be an N-polynomial and $\delta \in {F^*}_p$. Define

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

$$F_k(x) = (x^p - x + \delta)^{n_k} F_{k-1}\left(\frac{x^p - x}{x^p - x + \delta}\right), \qquad k \geq 1,$$

Then ${F^*}_k(x)$ is an N-polynomial of degree np^k over F_q if and only if

$$Tr_{q|p}\left(n + \frac{c_1}{c_0}\right) Tr_{q|p}(\delta \frac{\acute{P}(1)}{P(1)} - n\delta) \neq 0.$$

We present the proof of the theorem in Section 2.2 of Chapter 2.

In Part 2.3 by using Dickson's Theorem we construct families of irreducible polynomials of degree $4n^k$, (k = 1, 2,…) over a finite field of odd characteristics.

In the first we states Dickson's Theorem as follows.

Theorem 7 (Dickson). Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in F_q$ ($q = p^s$odd), where$c = \frac{1}{2}ab - \frac{1}{8}a^3$, then $f(x)$ is irreducible over F_q if and only if

$$(\frac{1}{2}b - \frac{1}{8}a^2)^2 - d \text{ , and } \frac{5}{16}a^4 - a^2b + 16d$$

are non-square inF_q.

Based on Dickson's Theorem, we discuss this problem. Let $P(x)$ be an irreducible polynomial of degree n over F_q, then it can be represented in F_{q^n} as $P(x) = \prod_{u=0}^{n-1}(x - \alpha^{q^u})$, for $\alpha \in F_{q^n}$. Substituting $x^4 + ax^3 + bx^2 + cx + d$ for x we obtain the polynomial $F(x)$ as

$$F(x) = P(x^4 + ax^3 + bx^2 + cx + d\ ) = \prod_{u=0}^{n-1}(x^4 + ax^3 + bx^2 + cx + d\ - \alpha^{q^u}).$$

Suppose $h(x) = x^4 + ax^3 + bx^2 + cx + d\ - \alpha$, then by Cohen's Theorem $F(x)$, is irreducible polynomial of degree $4n$ over F_q if and only if $h(x) \in F_{q^n}[x]$ be irreducible. But by Dickson's Theorem, $h(x)$ where $c = \frac{1}{2}ab - \frac{1}{8}a^3$ is irreducible if

and only if $X = (\frac{1}{2}b - \frac{1}{8}a^2)^2 - (d - \alpha) = -(T_1 - \alpha)$ and $Y = \frac{5}{16}a^4 - a^2b + 16(d - \alpha) = 16(T_2 - \alpha)$,

Where $T_1 = d - (\frac{1}{2}b - \frac{1}{8}a^2)^2$, and $T_2 = \frac{5}{16}a^4 - a^2b + d$, be non-square in

F_{q^n}. We know $X \in F_{q^n}$, is non-square if and only if $X^{\frac{q^n-1}{2}} = -1$. But we have

$$X^{\frac{q^n-1}{2}} = (-(T_1 - \alpha))^{\frac{q^n-1}{2}} = \{(-(T_1 - \alpha))^{\frac{q^n-1}{q-1}}\}^{\frac{q-1}{2}} = \prod_{u=0}^{n-1}\{(-(T_1 - \alpha))^{q^u}\}^{\frac{q-1}{2}}$$
$$= ((-1)^n P(T_1))^{\frac{q-1}{2}},$$

So $X \in F_{q^n}$, is non-square if and only if $((-1)^n P(T_1)) \in F_q$, be non-square. Like above relations it is clear that $Y \in F_{q^n}$, is non-square if and only if $P(T_1) \in F_q$, be non-square. First deduce the following theorem.

Theorem 8. Let $P(x)$ be an irreducible polynomial of degree n over F_q and $c = \frac{1}{2}ab - \frac{1}{8}a^3$. Then $F(x) = P(x^4 + ax^3 + bx^2 + cx + d)$ is irreducible of degree$4n$, if and only if $(-1)^n P(T_1)$, and $P(T_2)$, be non-square in F_q, where

$T_1 = d - (\frac{1}{2}b - \frac{1}{8}a^2)^2$, and $T_2 = \frac{5}{16}a^4 - a^2b + d$

We present the proof of the theorem in Section 2.3 of Chapter 2.

Now we apply above theorem to describe some recurrent methods for constructing families of irreducible polynomials over F_q our results are as follows:

(1) Let $b = d = 0$ *and* $a = c = 1$ and construct a recurrent method over F_{3^s}. By above notations in this case $T_1 = T_2 = 2$. Let

$$F_1(x) = F_0(x^4 + x^3 + x)$$

Where $F_0(x)$, is an irreducible polynomial of degree n over F_{3^s}. For irreducibility $F_1(x)$ by above Theorem we need that $(-1)^n F_0(2)$, and $F_0(2)$, are non-square inF_{3^s}. Namely n, is even and $F_0(2)$, be non-square in F_{3^s}. So we obtain this theorem by induction on k.

Theorem 9. Let $F_0(x)$ be an irreducible polynomial of degree n over F_{3^s}, where n is even. Suppose that $F_0(2)$, be non-square in F_{3^s}. Define

$$F_k(x) = F_{k-1}(x^4 + x^3 + x) \;\; k > 1,$$

then $F_k(x)$ is an irreducible polynomial of degree $n4^k$, over F_{3^s}.

We present the proof of the theorem in Section 2.3 of Chapter 2.

(2) Let$a = b = c = d = 0$, namely $F_1(x) = F_0(x^4)$, where $F_0(x)$ is an irreducible polynomial of degree n, over F_q. So in this case we have $T_1 = T_2 = 0$, then $F_1(x)$, is irreducible of degree $4n$ over F_q, if and only if $(-1)^n F_0(0)$, and $F_0(0)$, be non-square in F_q. It is equal that $F_0(0)$ be non-square and n is even when$q \equiv 3, (mod\ 4)$. By induction on$k$, we obtain this theorem.

Theorem 10. Let $F_0(x)$ be an irreducible polynomial of degree n over F_q, where n is even when $q \equiv 3, (mod\ 4)$. Suppose that $F_0(0)$, be non-square in F_q. Define

$$F_k(x) = F_{k-1}(x^4)\ \ k > 1,$$

then $F_k(x)$ is an irreducible polynomial of degree $n4^k$, over F_q.

We present the proof of the theorem in Section 2.3 of Chapter 2. Note by this theorem if we chose $F_0(x)$ as a trinomial (pentonomial) irreducible polynomial, so we derive a families of trinomial (pentonomial) irreducible polynomials, $F_k(x)$ over F_q of degree $n4^k$. These kind of irreducible polynomials are important in application.

(3) Let$a = c = d = 0$, namely $F_1(x) = F_0(x^4 + bx^2)$, so in this case we have $T_1 = -\frac{b^2}{4}$ and $T_2 = 0$. Then$F_1(x)$, is irreducible of degree $4n$, over F_q if and only if $(-1)^n F_0\left(-\frac{b^2}{4}\right)$ and$F_0(0)$, be non-square inF_q. By induction on$k$, we obtain this theorem.

Theorem 11. Let $F_0(x)$ be an irreducible polynomial of degree n over F_q, where n is even when$q \equiv 3, (mod\ 4)$. Suppose that $F_0(0)$ and $F_0\left(-\frac{b^2}{4}\right)$, be non-square in F_q and $b^6 + 16b^3 + 64 = 0$. Define

$$F_{k+1}(x) = F_k(x^4 + bx^2), k > 1$$

then $F_k(x)$ is an irreducible polynomial of degree $n4^k$, over F_q.

We present the proof of the theorem in Section 2.3 of Chapter 2.

Chapter 3 includes a factorization of some composition polynomials when assumptions on the Cohen's Theorem fail to hold by using M. Kyuregyan and G. Kyuregyan's Theorem over F_q and by writing some programs we determine all their irreducible factors. On the other hand we factorize these composition polynomials where $P(x)$ is an irreducible polynomial of degree n over F_q.

1) $\left(dx^{q^n} - rx + h\right)^n P\left(\frac{ax^{q^n} - bx + c}{dx^{q^n} - rx + h}\right)$,

2) $(dx^q - rx + h)^n P\left(\frac{ax^q - bx + c}{dx^q - rx + h}\right)$.

The main theorems of this part are as follows:

Theorem 12. Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over F_q and $\delta_0, \delta_1 \in F_q$, $\delta_0 \neq \delta_1$. Then

$$F(x) = \left(x^{q^n} - x + \delta_1\right)^n P\left(\frac{x^{q^n} - x + \delta_0}{x^{q^n} - x + \delta_1}\right)$$

decompose as a product of $\frac{q^n}{p}$ irreducible polynomials of degree np over F_q.

We present the proof of the theorem in Section 3.1 of Chapter 3.

Theorem 13. Let$\delta_0, \delta_1, \delta_2 \in F_q$, $\delta_0 \neq \delta_1, \delta_2 \neq 0,1$. Suppose that $P(x)$ be an irreducible polynomial of degree n over F_q. Then the polynomial

$$F(x) = \left(x^{q^n} - \delta_2 x + \delta_1\right)^n P\left(\frac{x^{q^n} - \delta_2 x + \delta_0}{x^{q^n} - \delta_2 x + \delta_1}\right)$$

decompose as a product of one irreducible polynomial of degree n and $\frac{q^n - 1}{t}$ irreducible polynomials of degree nt over F_q where$t = ord(\delta_2)$.

We present the proof of the theorem in Section 3.1 of Chapter 3.

Theorem 14. Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over F_q and $\delta_0, \delta_1 \in F_q, \delta_0 \neq \delta_1$. Suppose that

$$n\delta_1 + (\delta_0 - \delta_1)\frac{P'(1)}{P(1)} = 0.$$

Then

$$F(x) = (x^q - x + \delta_1)^n P\left(\frac{x^q - x + \delta_0}{x^q - x + \delta_1}\right),$$

is decomposed as a product of q irreducible polynomial of degree n Over F_q.

We present the proof of the theorem in Section 3.2 of Chapter 3.

Theorem 15. Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over F_q and $\delta_0, \delta_1 \in F_q, \delta_0 \neq \delta_1$. Suppose that

$$n\delta_1 + (\delta_0 - \delta_1)\frac{P'(1)}{P(1)} \neq 0$$

Then

$$F(x) = (x^q - x + \delta_1)^n P\left(\frac{x^q - x + \delta_0}{x^q - x + \delta_1}\right),$$

is decomposed as a product of $\frac{q}{p}$ irreducible polynomial of degree np over F_q.

We present the proof of the theorem in Section 3.2 of Chapter 3.

Theorem 16. Let $\delta_0, \delta_1, \delta_2 \in F_q$, $\delta_0 \neq \delta_1, \delta_2 \neq 0,1$. Suppose that $P(x)$ be an irreducible polynomial of degree n over F_q and $\gcd(n, q-1) = 1$. Then the composite polynomial

$$F(x) = (x^q - \delta_2 x + \delta_1)^n P\left(\frac{x^q - \delta_2 x + \delta_0}{x^q - \delta_2 x + \delta_1}\right),$$

factors as a product of one irreducible polynomial of degree n and $\frac{q-1}{t}$ irreducible polynomial of degree nt over F_q where $t = ord(\delta_2)$.

We present the proof of the theorem in Section 3.2 of Chapter 3.

In Chapter 4, we focused on arithmetics in finite fields specially multiplication.

Let A and B be two elements of F_{2^m} and represented with respect to the NB as

$$A = \sum_{i=0}^{m-1} a_i \beta^{2^i} \quad and \quad B = \sum_{i=0}^{m-1} b_i \beta^{2^i}.$$

Let C denote their product

as

$$C = AB = \left(\vec{a} \times \overrightarrow{\beta^T}\right) \times \left(\vec{\beta} \times \overrightarrow{b^T}\right) = \vec{a} \times M \times \overrightarrow{b^T},$$

where the multiplication matrix M is defined by

$$M = \overrightarrow{\beta^T} \times \vec{\beta} = \left[\beta^{2^i+2^j}\right].$$

One can see that

$$c_i = \overrightarrow{a^{(i)}} \times M_0 \times \overrightarrow{b^{(i)^T}}, \quad 0 \le i \le m-1,$$

Where $\overrightarrow{a^{(i)}} = [a_i, a_{i+1}, \dots, a_{i-1}]$ and $\overrightarrow{b^{(i)}} = [b_i, b_{i+1}, \dots, b_{i-1}]$ are respectively, the $i - fold$ left cyclic shift of a and b. Also if we set

$$\beta\beta^{2^j} = \sum_{k=0}^{m-1} \gamma_{jk}\beta^{2^k},$$

then $(\gamma_{j0}, \gamma_{j1}, \dots, \gamma_{j,m-1})$ is the $j - th$ row of matrix M_0. The numbers of 1s in the component Matrix M_0 is known as the complexity of the normal basis.

Let $P(x)$ be an N-polynomial of degree n over F_q and α is some root of $P(x)$ in F_{2^n}. Set a standard basis of form

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\},$$

to present each element

$$\alpha.\alpha, \alpha.\alpha^2, \alpha.\alpha^{2^2}, \dots, \alpha.\alpha^{2^{n-1}}.$$

In this basis, each element in the field F_{2^n} can be represented by n binary digits. So we set

$$(A)_1 = \alpha.\alpha = \alpha^2 = (0,0,1,0, \dots,0),$$

$$(A)_2 = \alpha.\alpha^2 = \alpha^3 = (0,0,0,1,0, \dots,0),$$

$$\vdots$$

$$(A)_n = \alpha.\alpha^{2^{n-1}} = \alpha^3 = (\dots),$$

as rows of the matrix $A_{n\times n}$. Also define

$$(P)_1 = \alpha = (0,1,0, \dots,0),$$

$$(P)_2 = \alpha^2 = (0,0,1,0, \dots,0),$$

$$\vdots$$

$$(P)_n = \alpha^{2^{n-1}} = (\dots),$$

as rows of the matrix $P_{n\times n}$.From linear algebra it can be derived that $M_0 = AP^{-1}$, where the number of non-zero entries in M_0 is equal to the complexity of normal basis of constructed by N-polynomial of $P(x)$. In Chapter 4 by using this method we compute complexity of families of N-polynomials over F_2 and F_3.

Main results of the dissertation are the following

1) Using Q-Transformation over F_{3^s} as follows

$$F_{k+1}(x) = F_k{}^Q(x) = x^{n2^{k-1}} F_k(x + \delta^2 x^{-1}), \quad k \geq 1,$$

and introduce families of self-reciprocal irreducible polynomials and N-polynomials over F_{3^s}.

2) Producing a new recurrent method for constructing families of N-polynomials over F_q of the degree np^k as follows:

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

$$F_k(x) = (x^p - x + \delta)^{n_k} F_{k-1}\left(\frac{x^p - x}{x^p - x + \delta}\right), \qquad k \geq 1,$$

3) By using Dickson's Theorem we construct families of irreducible polynomials of degree $4n^k, (k = 1,2, \dots)$ over a finite field of odd characteristics.

4) Factorization of some composite polynomials over finite fields and obtains their irreducible factors.

Publications of results of dissertation

[1] S. Mehrabi, Recurrent Methods for Constructing Irreducible Polynomials over F_q of Odd Characteristics, International Mathematical Forum, Vol. 7, 2012, no. 24, 1171 - 1177

[2] S. Maharbi, Factorization of composite polynomials over finite fields, Turk J Math, doi: 10.3906/mat-1201-53, (Received: 28.01.2012, Accepted: 01.10.2012.)

[3] S. Mehrabi, On the Reducibility of Some Composite Polynomials over Finite Fields, Gen. Math. Notes, Vol. 10, No. 1, May 2012, pp.51-57

[4] M. Alizadeh, S. Abrahamyan, S. Mehrabi, M. K. Kuyregyan, Constructing N-Polynomials over Finite Fields, International Journal of Algebra, Vol. 5, 2011, no. 29, 1437 - 1442

[5] S. Mehrabi, M. K. Kyuregyan, Composition of irreducible polynomials, CSIT Conference 2011, Yerevan, Armenia, September 26-30, pp.155-156.

[6] S. Mehrabi, A new recurrent method for constructing irreducible polynomial over finite fields of characteristic three, CSIT Conference 2011, Yerevan, Armenia, September 26-30, pp.153-154.

Սաիդ Մեհրաբի

Ամփոփում

Վերջավոր դաշտերի վրա Անվերածելի և նորմալ բազմանդամների ռեկուրսիվ կառուցումներ

Աշխատանքը վերաբերվում է վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների կառուցմանը: Վերջավոր դաշտերի վրա տրված անվերածելի և նորմալ բազմանդամները մեծ հետաքրքրություն են ներկայացնում և տեսական, և կիրառական խնդիրներում: Այս աշխատանքում ներկայացված են F_q դաշտի վրա անվերածելի բազմանդամների որոշակի դասեր կառուցելու համար նոր ռեկուրենտ եղանակներ: Ավելին մենք ցույց ենք տվել, որ որոշ պայմանների դեպքում այս անվերածելի բազմանդամները հանդիսանում են նորմալ բազմանդամներ: Մենք նաև դիտարկել ենք որոշ կոմպոզիցիոն բազմանդամների վերլուծությունը, երբ Կոհենի թեորեմի ենթադրությունը տեղի չունի և որոշակի ծրագրի միջոցով մենք գտնում ենք բոլոր անվերածելի արտադրիչները: Վերջում մենք քննարկել ենք վերջավոր դաշտերի տեսության առանձնահատկությունները, մասնավորապես վերջավոր դաշտերի վրա բազմապատկման գործողության կարևորությունը և ցույց ենք տվել, թե ինչու են նորմալ բազմանդամները կարևոր բազմապատկման գործողության ժամանակ: Այնուհետև դիտարկվել է նորմալ բազիսների բարդությունը և օգտագործելով էֆֆեկտիվ մեթոդ, մենք հաշվել ենք մեր կողմից ստացված նորմալ բազմանդամների բարդությունները:

Թեզում ստացված հիմնական արդյունքները բերված են ստորև

1. F_{3^s} դաշտի վրա օգտագործելով

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

Q-ձևափոխություն (Q-Transformation)–ը, ստանում ենք ինքնաերկակի անվերածելի և նորմալ բազմանդամների ընտանիք F_{3^s} դաշտի վրա հետևյալ թեորեմի միջոցով.

Թեորեմ Դիցուք $q = 3^s$, որտեղ s զույգ թիվ է և $F_1(x) = x^2 + bx + \delta^2$ քառակուսային բազմանդամ է F_{3^s} դաշտի վրա, b և δ-ն ոչ զրոյական էլեմենտներ են և $b^2 - \delta^2$ ոչ քառակուսային էլեմենտ է F_{3^s} դաշտում:

Ռեկուրսիվ ձևով սահմանենք $F_k(x)$ հաջորդականությունը հետևյալ ձևով.

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

Այդ դեպքում $(F_k(x))_{k\geq 1}$ հաջորդականության յուրաքանչյուր անդամ հանդիսանում է $t_k = 2^k$ աստիճանի համատեղելի հետքով(trace-compatible) նորմալ բազմանդամ: Ավելին, եթե α_k–ն բազմանդամի արմատն է, ապա α_k–ն հանդիսանում է $F_{3^{snk}}$ դաշտի լիովին նորմալ էլեմենտ F_{3^s} դաշտի վրա [6].

2. Առաջարկվել է $n \cdot p^k$ $k \geq 1$ աստիճանի նորմալ բազմանդամների կառուցման նոր ռեկուրենտ մեթոդ F_q դաշտի վրա հետևյալ կոմպոզիցիոն եղանակի միջոցով [4]:

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

$$F_k(x) = (x^P - x + \delta)^{n_{k-1}} F_{k-1}\left(\frac{x^P - x}{x^P - x + \delta}\right) \quad k \geq 1.$$

3. Օգտագործելով Դիկսոնի թեորեմը, մենք կառուցել ենք $4 \cdot n^k$ աստիճանի անվերածելի բազմանդամների հաջորդականության կենտ բնութագրիչ ունեցող դաշտերի համար [1,5].

4. Տրվել է որոշակի կոմպոզիցիոն բազմանդամների վերլուծությունը վերջավոր դաշտերի վրա և ստացվել է նրանց անվերածելի արտադրիչները հետևյալ ձևով [2,3].

$$\left(dx^{q^n} - rx + h\right)^n P\left(\frac{ax^{q^n} - bx + c}{dx^{q^n} - rx + h}\right)$$

$$(dx^q - rx + h)^n P\left(\frac{ax^q - bx + c}{dx^q - rx + h}\right)$$

ЕЗЮМЕ

САИД МЕГРАБИ

РЕКУРСИВНОЕ ПОСТРОЕНИЕ НЕПРИВОДИМЫХ И НОРМАЛЬНЫХ ПОЛИНОМОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Работа посвящена построению неприводимых и нормальных полиномов над конечными полями. Неприводимые и нормальные полиномы, заданные на конечных полях, представляют большой интерес и в теоретических, и в прикладных задачах. В данной работе мы представляем некоторые новые рекуррентные методы для построения определенных новых классов неприводимых полиномов на поле F_q. Более того, мы показали, что в определенных условиях эти неприводимые полиномы являются нормальными полиномами. Мы также проанализировали некоторые композиционные полиномы, когда предположение теоремы Коэна не имела места, и с помощью определенной программы нашли все неприводимые множители. В конце мы обсудили арифметику теории конечных полей, в частности действие умножения на конечных полях, и показали почему важны нормальные полиномы во время действия умножения. Затем была рассмотрена сложность нормальных базисов, и мы рассчитали сложности полученных нами нормальных полиномов, используя эффективный метод.

Основные результаты, полученные в тезисе, приведены ниже:

1- Используя Q-преобразование (Q-Transformation) на поле F_{3^s},

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

получаем самодвойственное семейство неприводимых и нормальных полиномов на поле F_{3^s} при помощи следующей теоремы.

Теорема. Допустим $q = 3^s$, где s - четное число, и $F_1(x) = x^2 + bx + \delta^2$ – квадратный полином на поле F_{3^s}, b и δ - ненулевые элементы и $b^2 - \delta^2$ - не квадратный элемент на поле F_{3^s}.

Определим рекурсивным методом последовательность $F_k(x)$ следующим образом:

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

В этом случае каждый член последовательности $(F_k(x))_{k\geq 1}$ является trace-compatible нормальным полиномом степени $t_k = 2^k$. Более того, если α_k - корень полинома $F_k(x)$, тогда α_k является полностью нормальным элементом поля $F_{3^{snk}}$ на поле F_{3^s} [6].

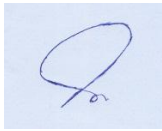
2- Был предложен новый рекуррентный метод построения нормальных полиномов степени $n \cdot p^k \; k \geq 1$ на поле F_q при помощи следующего композиционного метода [4]:

$$F_0(x) = P(x)$$
$$F_k(x) = (x^P - x + \delta)^{n_{k-1}} F_{k-1}\left(\frac{x^P - x}{x^P - x + \delta}\right) \quad k \geq 1.$$

3- Используя теорему Диксона, мы построили последовательность неприводимых полиномов степени $4 \cdot n^k$ для полей, имеющих нечетную характеристику [1,5].

4- Был дан анализ некоторых композиционных полиномов на конечных полях и получены их неприводимые множители следующим образом [2,3]:

$$\left(dx^{q^n} - rx + h\right)^n P\left(\frac{ax^{q^n} - bx + c}{dx^{q^n} - rx + h}\right)$$
$$(dx^q - rx + h)^n P\left(\frac{ax^q - bx + c}{dx^q - rx + h}\right)$$



Ծավալը - 1 տ.մ. Տպաքանակը - 100 օրինակ

Տպագրված է ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային

պոլիգրաֆիայի լաբորատորիայում