ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ
ԻՆՍՏԻՏՈՒՏ

ՄԱՀՄՈՒԴ ԱԼԻԶԱԴԵՀ

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՎՐԱ ԱՆՎԵՐԱԾԵԼԻ ԵՎ ՆՈՐՄԱԼ ԲԱԶՄԱՆԴԱՄՆԵՐԻ 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

MAHMOOD ALIZADEH

CONSTRUCTION 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. 15:00-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.
Մաասնագիտական 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 15:00 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 IIAP.

Author’s abstract is sent on 2 September, 2013.

Scientific secretary of the specialized council,

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

1. GENERAL CHARACTERIZATION OF THESIS

Actuality of the subject

The theory of finite fields is a branch of modern algebra that has come to the fore in the last 50 years because of its diverse application in combinatorics, coding theory, and mathematical study of switching circuits, among others. The origins of the subject reach back into the 17^{th} and 18^{th} century, with such eminent mathematicians as Pierre de Fermat(1601-1665), Leonhard Eular (1707-1738), Joseph-Louis Lagrange (1736-1813), and Adrien-Marie Legendre(1752-1833) contributing to the structure theory of special finite fields namely, the so-called finite prime fields. The general theory of finite fields may be said to begin with the work of Carl Friedrich Gauss (1777-1855) and Everiste Galois (1811-1832), but it only became of interest for applied mathematicians in recent decades with the emergence of discrete mathematics as a serious discipline. In parallel with the development of the theory of finite fields there was a rapid growth of polynomial theory based on finite fields. The finite fields based theory is important not only for the study of algebraic structures on finite fields, but it has many other applications, such as, coding theory and cryptography. Moreover, the irreducible and normal polynomials play a special role in this, as they are necessary in construction of finite fields and in procedures with the elements of the field.

There are two methods for constructing irreducible (or normal) polynomials over finite fields. The first method is the polynomial composition method that allows constructions of irreducible (or normal) polynomials of higher degree from given irreducible (or normal) polynomials over finite fields. The second method is the testing method for irreducibility and normality of the polynomials over finite fields. The first method has been studied by Varshamov[1], Cohen[2], Kyuregyan[3] and others. The second method has been studied by several authors, including Ben-Or[4], Rabin[5]. The elements in a normal basis are exact roots of an *N*-

---

[1] R. R. Varshamov, "*A general method of synthesizing irreducible polynomials over Galois fields*", Soviet Math. Dokl., no. 29, pp. 334 – 336, 1984.

[2] S. D. Cohen, "*Explicit theorems on generator polynomials*", Finite Fields Appl., no. 11, pp. 337-357, 2005.

[3] M. K. Kyuregyan, "*Recurrent methods for constructing irreducible polynomials over* $GF(2^s)$", Finite Fields Appl. No. 8, pp. 52-68, 2002.

[4] M. Ben-Or, "*Probabilistic algorithms in finite fields*", IEEE, CH1695-6/81/0000/0394$OO.7, 1981.

polynomial. Hence an N-polynomial is just another way of describing a normal basis. The growing interest towards normal bases is due to their theoretical and practical importance. Already in 1888, Hensel[6] has remarked, certain advantages of constructing finite fields based on normal polynomials. The problem was predetermined by Gao[7] in 19th century.

In hardware devices (chips) and software packages the complexity of the procedures over finite fields is determined by the selection of normal base. The algorithm of Messi-Omura[8] can be served as a proof of the above mentioned.

It is well known that when using normal bases, the speed of multiplications over F_q depends directly on the complexity of normal basis. And, it is important to use a normal basis in F_q , with the lowest possible complexity. When no optimal normal basis exists, the problem of classifying of all the low complexity normal bases stays open. This problem has been studied by several authors, including, Jungnickel[9], Masuda[10]. Construction of irreducible and normal polynomials (with the lowest possible complexity) is an important problem in finite fields. This thesis is devoted to the construction of irreducible and normal polynomials (with their complexities) over finite fields.

The Aim of the Thesis

The aim of the thesis is described below.

1. Research recursive methods for constructing irreducible and normal polynomials over finite fields.
2. Propose new approaches for polynomial construction.
3. Give a complete factorization of some composite polynomials.
4. Study investigation methodologies for discovering normal bases over finite fields.

---

[5] M. O. Rabin, "*Probabilistic algorithms in finite fields*". SIAM J. Comp. 9 (1980), 273-280.

[6] K. Hensel, "*über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*", J. Reine Angew. Math., no. 103, pp. 230-237, 1888.

[7] S. Gao, "*Normal bases over finite fields*", Ph.D. Thesis, Waterloo, 1993.

[8] J. L. Massey and J. K. Omura, "*Computational method and apparatus for finite field arithmetic*", U.S. patent no. 4, pp. 587-627, May 1986.

[9] D. Jungnickel, "*Trace-orthogonal normal basis*", Discrete Applied Mathematics. no. 47, pp. 233-249, 1993.

[10] A. M. Masuda, L. Moura, D. Panario, D. Thomson, "*Low Complexity Normal Elements over Finite Fields of Characteristic Two*", IEEE Trans. Comput., no. 57, pp. 990-1001, 2008.

5. Propose new algorithms based on existing results for testing normality of given irreducible polynomials and computing the complexity of the given normal polynomials over finite fields.

Approbation

The results of the work have been presented in 8^{th} International Conference "Computer Science and Information Technologies" CSIT-2011, (September 26-30, 2011, Yerevan, Armenia).

Object of Investigation

The objects of investigation are irreducible and normal polynomials over finite fields.

Methods of Investigation

The methods of finite field theory, linear algebra, implementation of finite field arithmetic and programming in the Matlab environment have been used.

Scientific novelty

1. Novel methods are proposed for irreducible polynomial construction and complete factorization of some composite polynomials, where
$$F(x) = (x^p - rx + h)^n P\left(\frac{x^p - bx + c}{x^p - rx + h}\right),$$
composition method is proposed.
2. A new method is suggested for explicit construction of normal polynomials, given composition method
$$F(x) = (x^p - x + h)^n P\left(\frac{x^p - x}{x^p - x + h}\right).$$
3. Efficient algorithms are found based on theoretical results for testing normality of the given irreducible polynomials and computing the complexity of given normal polynomials. In some tables, the complexity of some recursive constructed normal polynomials is computed. Also a list of all normal polynomials of degree n over F_p, with their complexities for some small values of n and $p,$ and a table of all normal polynomials with minimum complexity of degree n over F_p for $p^n \leq 10^7$, and $p \leq 7$, are obtained.

Practical significance

The results of this thesis are useable in the some applications including, coding theory and cryptography.

Publications

The results of the thesis were published in five scientific articles which are listed in "List of Publications".

Structure and Volume of the Thesis

The thesis consists of introduction, three chapters, conclusion and the list of references. The number of references is 65. The volume of the work is 96 pages.

2. THE MAIN CONTENT OF THE THESIS

In Chapter 1**,** the actuality of the topic is discussed; the aim and the problems of the dissertation are formulated. In this chapter, also the necessary definitions and the previous results related to the subject of the thesis are shortly presented. In Chapter 2, a new recursive method for constructing irreducible polynomials of degree $np^k (k \geq 1)$ over F_q, by using an irreducible polynomial of degree n is given. Also in this chapter, we provide a proof for two theorems of Varshamov[11], which had been stated by him in 1973, without proof, and are proved by Kyuregyan[12] for some special cases in 2011. We use of an analogous technique, which used by Kyuregyan. In chapter 3, by using a composition method, a new recursive construction method for normal polynomials of degree $np^k (k \geq 1)$, using a normal polynomial of degree n is given. In chapter 4, two algorithms have been developed. The first, tests normality of irreducible polynomials of degree n (which uses $O\big(nM(n)(n\log(q)+\log(n))\big)$ operations in F_q), and the second one, compute the complexity of normal polynomials of degree n (that uses $O\big(n(n^2 + M(n)\log(qn))\big)$ operations in F_q , (when $M(n) = n\log(n)\log(\log(n))$ and the arithmetic is based on FFT (Fast Fourier Transform)). Also in this chapter some results of these algorithms in some tables are given.

---

[11] R. R. Varshamov, “ *Operator substitutions in a Galois field and their applications*”, Dokl. Akad. Nauk SSSR, no. 211, pp. 768-771, 1973.

[12] M. K. Kyuregyan and G. M. Kyureghyan “ *Irreducible compositions of polynomials over finite fields*”, Designs, Codes and Cryptography, no. 61, vol. 3, pp. 301-314, 2011.

Bellow is brought summary of results obtained in the thesis.

Chapter 2: Construction of irreducible polynomials over finite fields

- Let for a prime power $q = p^s (s \in N)$ and a positive integer $n \geq 2$, F_q be the finite fields with q elements and F_{q^n} be its extension of degree n. The *trace* of $\alpha \in F_{q^n}$ over F_q is defined by

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}.$$

- The polynomial $P(x) \in F_q[x]$ is called *irreducible* over F_q if $P(x) = r(x)\, h(x)$ implies that $r(x)$ or $h(x)$ is any non zero constant of F_q.

Theorem 2.1 Let $x^p - \delta_2 x + \delta_0$ and $x^p - \delta_2 x + \delta_1$ be relatively prime polynomials in $F_q[x]$ and $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over F_q of degree $n \geq 2$, and let $\delta_0, \delta_1 \in F_q$, $\delta_2 \in F_q^*, \delta_0 \neq \delta_1$. Then

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

is an irreducible polynomial of degree np over F_q if and only if ${\delta_2}^{\frac{q-1}{p-1}} = 1$ and

$$Tr_{q|p}\left(\frac{1}{A^p}\left((\delta_1 - \delta_0)\frac{P'(1)}{P(1)} - n\delta_1\right)\right) \neq 0,$$

where $A^{p-1} = \delta_2$, for some $A \in F_q^*$.

Theorem 2.2 Let $x^p - x + \delta_0$ and $x^p - x + \delta_1$ be relatively prime polynomials in $F_q[x]$ and $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over F_q of degree $n \geq 2$ and let $\delta_0, \delta_1 \in F_q$, $\delta_0 \neq \delta_1$. Suppose that

$$Tr_{q|p}\left((\delta_1 - \delta_0)\frac{P'(1)}{P(1)} - n\delta_1\right) = 0.$$

Then the polynomial

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

factors to p irreducible polynomials of degree n over F_q as follows:

$$F(x) = G_0(x) G_1(x) \; \dots \; G_{p-1}(x).$$

Moreover let denote

$$H_i(x) = (x^p - x + \delta_1)^n \, G_i \left(\frac{x^p - x + \delta_0}{x^p - x + \delta_1}\right), \qquad 0 \le i \le p-1.$$

If gcd(n,p)=1, then $G_0(x), G_1(x), \ldots, G_{p-1}(x)$ are pairwisely different. Also exactly one of the polynomials $H_0(x), H_1(x), \ldots, H_{p-1}(x)$ factors to p irreducible polynomials of degree n over F_q and the others are pairwisely different irreducible polynomials of degree np over F_q.

The following theorem had been stated by Varshamov without proof (1973). In the case $e = q^m - 1$, the following theorem is proved by M. K. Kyuregyan and G. M. Kyuregyan. We provide a proof for it, in general case, using an analogues technique which used by Kyuregyan.

Theorem 2.3 Let $\gcd(n, e) = 1$ and let $l(x) = \sum_{v=0}^{m} b_v x^{q^v}$ such that its conventional *q-associate* $\bar{l}(x) \neq x - 1$ is a monic irreducible polynomial of degree m over F_q belonging to order e. Further, let $f(x)$ be a monic irreducible polynomial of degree n over F_q and $\Psi(x)$ be the minimal polynomial of $l(\alpha)$, where $\alpha \in F_{q^n}$ is a root of $f(x)$. Then the polynomial

$$F(x) = \frac{\Psi\big(l(x)\big)}{f(x)},$$

decomposes as a product of $e^{-1}(q^m - 1)$ distinct irreducible polynomials of degree ne over F_q.

Theorem 2.4 Let $\beta, \gamma \in F_q$, $\beta \neq -\gamma$ and $f(x) \neq x - 1$ be an irreducible polynomial of degree n over F_q belonging to order e. Then the polynomial

$$F(x) = (x + \gamma)^n f\left(\frac{x^{q^n} - \beta}{x + \gamma}\right),$$

decomposes as a product of one irreducible polynomial of degree n and $e^{-1}(q^n - 1)$ irreducible polynomials of degree ne over F_q.

The above theorem, for the case $e = q^n - 1$ is proved by M. K. Kyuregyan and G. M. Kyuregyan. We provide a proof for it, in general case, using an analogues technique which used by Kyuregyan.

Theorem 2.5 Let $x^p - x + \delta$ and $x^p - x + 1$ be relatively prime polynomials in $F_p[x]$ and $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over F_p of degree $n \geq 2$. Let also $\delta \in F_p$, $\delta - 1 \neq 0$.

Define

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

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

where $t_k = np^k$ denotes the degree of $F_k(x)$. Suppose that

$$\Big((\delta - 1)F_0'(1) + nF_0(1)\Big).\Big((\delta - 1)F_0'(\delta) - nF_0(\delta)\Big) \neq 0.$$

Then $(F_k(x))_{k\geq 0}$ is a sequence of irreducible polynomials over F_p of degree $t_k = np^k$, for every $k \geq 0$.

Chapter 3: Construction of normal polynomials over finite fields

- **A** *normal* basis of F_{q^n} over F_q is a basis of the form $N = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$, i.e., a basis that consists of the algebraic conjugates of a fixed element $\alpha \in F_q^*$.
- A monic irreducible polynomial $F(x) \in F_q[x]$ is called *normal polynomial* or *N-polynomial* if its roots form a normal basis or, equivalently, if they are linearly independent over F_q.

Theorem 3.1 Let $P(x) = \sum_{i=0}^{n} c_i x^i$, with $P(x) \neq x$ be an *N*-polynomial over F_q of degree n and let $\delta \in F_q^*$. Also let

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

Then $F^*(x)$ is an *N*-polynomial of degree np over F_q if

$$\left(n + \frac{P^{*'}(0)}{P^*(0)}\right) Tr_{q|p}\left(\delta \frac{P^{*'}(1)}{P^*(1)} - n\delta\right) \neq 0.$$

Theorem 3.2 Let $P(x)$, with $P(x) \neq x$ be an *N*-polynomial of degree n over F_q. Define

$$F_0(x) = P^*(x)$$
$$F_k(x) = (x^p - x + \delta)^{np^{k-1}} F_{k-1}\left(\frac{x^p - x}{x^p - x + \delta}\right), \quad k \geq 1,$$

where $\delta \in F_p^*$. Then $(F_k^*(x))_{k\geq 0}$ is a sequence of *N*-polynomials of degree np^k over F_q if

$$Tr_{q|p}\left(n + \frac{P^{*'}(0)}{P^*(0)}\right) Tr_{q|p}\left(\frac{P^{*'}(1)}{P^*(1)} - n\right) \neq 0,$$

where $P^{*'}(0)$ and $P^{*'}(1)$ are formal derivatives of $P^*(x)$ at the points 0 and 1, respectively.

Chapter 4: Implementation of finite fields arithmetic

Let $N = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Then for any $i, j, 0 \le i, j \le n-1$, $\alpha_i \alpha_j$ is a linear combination of $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ with coefficients in F_q. In particular,

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = T \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix},$$

where T is an $n \times n$ matrix over F_q. The matrix T is called the *multiplication table* of the normal basis N. If α is a normal element, the multiplication table of the normal basis generated by α is also referred as the multiplication table of α. The number of non-zero entries in T is called the *complexity* of normal basis N, denoted by c_N. Recall that for any normal basis N of F_{q^n} over F_q, $c_N \ge 2n-1$. A normal basis N is called *optimal* if $c_N = 2n-1$.

It is well known that when using normal basis, the speed of multiplications in F_{q^n} depends directly on the complexity of normal basis. And, it is important to use a normal basis in F_{q^n}, with the lowest possible complexity. When no optimal normal basis exists, the problem of classifying of all low complexity normal bases stays open.

There are some normality testing of irreducible polynomials, which need to some complex computing and are not efficiently for big degrees polynomials. An efficient method for normality testing of field elements (for binary fields) is discussed by Masuda in 2008. Masuda's algorithm is based on the following theorem.

Theorem (Gao): The irreducible polynomial $P(x)$ of degree n over F_q is an *N*-polynomial if and only if $gcd\left(\sum_{i=0}^{n-1} \alpha^{q^i} x^i, x^n - 1\right) = 1$ (in F_{q^n}[x]), where $\alpha \in F_{q^n}$ is a root of $P(x)$.

Masuda's algorithm needs a lot of computations in F_{q^n}[x], for normality testing of an element in F_{q^n} (only with characteristic two). We give an efficient algorithm for normality testing of irreducible polynomials over finite fields with characteristic p (for each prime p), based on the following theorem, which needs to computations in F_q[x].

Theorem (Gao): The irreducible polynomial $P(x)$ of degree n over F_q is an *N*-polynomial if and only if $gcd\left(\sum_{i=0}^{n-1} t_i x^i, x^n - 1\right) = 1$ (in F_q[x]), where $t_i = Tr_{q^n|q}(\alpha\alpha^{q^i})$ for $0 \le i \le n-1$ and $\alpha \in F_{q^n}$ is a root of $P(x)$.

All of traces and powers of α, in our algorithm are computed by repeated squaring method. Our algorithm uses $O\big(nM(n)(n\log(q)+\log(n))\big)$ operations in F_q, when $M(n)=n\log(n)\log(\log(n))$, and efficiently tests normality of each irreducible polynomial of degree n over F_p, for each integer n and prime p, since all computations for testing are in F_p[x]. Also in the continue an algorithm for computing the complexity of a normal polynomial, that uses $O\big(n(n^2+M(n)\log(qn))\big)$ operations in F_q, is given.

Using these algorithms and some given recursive methods for constructing normal polynomials some programs in the matlab environment are created. Using these programs we will compare some normal polynomials constructed by Theorem 3.2 and some previously known methods. We also list a set of all normal polynomials of degree n over F_p, with their complexities for a small value of n and p ($p=2; n\leq 11,\ p=3; n\leq 7, p=5;\ n\leq 5, p=7; n\leq 4$). Finally we give a table of all normal polynomials with minimum complexity of degree n over F_p for $p^n\leq 10^7$, and $p\ \leq 7$.

3. THE MAIN RESULTS OF THE THESIS

In this thesis, several methodologies for constructing irreducible and normal polynomials over finite fields are studied; new algorithms based on some theoretical results for testing normality of the given irreducible polynomials and computing complexity of the given normal polynomials are found. The main results of the thesis are brought below.

- A recursive method for constructing irreducible polynomials of degree np^k $(k\geq 1)$ over finite fields has been carried out, using the polynomial composition

$$F(x)=(x^p-\delta_2x+\delta_1)^nP\left(\frac{x^p-\delta_2x+\delta_0}{x^p-\delta_2x+\delta_1}\right),$$

where $P(x)$ is an irreducible polynomial of degree n over F_q [2].

- Factorization of some polynomial compositions have been studied, including,

$$F(x)=(x^p-x+\delta_1)^nP\left(\frac{x^p-x+\delta_0}{x^p-x+\delta_1}\right),$$

where $P(x)$ is an irreducible polynomial of degree n over F_q, and

$$F(x)=\frac{\Psi\big(l(x)\big)}{f(x)},$$

for irreducible polynomials $f(x)$ and $\bar{l}(x)$ of degrees n and m respectively, such that $l(x)$ is the linearized q-associated of $\bar{l}(x)$ [1].

- A recursive method for normal polynomial construction of degree $np^k\ (k \geq 1)$ was developed (over finite fields), using the polynomial composition

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

where $P(x)$ is an irreducible polynomial of degree n over F_q [3].

- Two algorithms have been developed. The first, tests normality of irreducible polynomials over F_q (which uses $O(nM(n)(nlog(q) + \ log(n)))$ operations in F_q), and the second one, computes the complexity of normal polynomials over F_q (which uses $O\big(n(n^2 + M(n)\log(qn))\big)$ operations in F_q). Using these algorithms, we compare complexity of some normal polynomials constructed by some recursive methods. In addition, we list the set of all normal polynomials of degree n over F_q, with their complexities for values of n and p ($p = 2;\ n \leq 11, p = 3;\ n \leq 7, p = 5;\ n \leq 5, p = 7;\ n \leq 4$). Finally, all normal polynomials of minimum complexity of degree n over F_p for $p^n \leq 10^7$, and $p \leq 7$ have been listed [4-5].

List of Publications

[1] M. Alizadeh, M. K. Kyuregyan, Factorization of some composite polynomials over finite fields, Journal of Algebra and Its Applications, Vol. 12, No. 3, 1250180 (6 pages), 2013.

[2] S. Abrahamyan, M. Alizadeh, M. K. Kyureghyan, Recursive constructions of irreducible polynomials over finite fields, Finite Fields and Their Applications, No. 18, pp. 738-745, 2012.

[3] M. Alizadeh, S. Abrahamyan, S. Mehrabi, M. K. Kyuregyan, Constructing N-Polynomials over Finite Fields, Proceedings of 8th International conference on Computer Science and Information Technologies (CSIT 2011), pp. 100-103, 2011.

[4] M. Alizadeh, Some Algorithms for Normality Testing Irreducible Polynomials and Computing Complexity of the Normal Polynomials over Finite Fields, Applied Mathematical sciences, Vol. 6, No. 40, pp. 1997-2003, 2012.

[5] M. Alizadeh, Computing of the Complexity of some Recursive Constructed Normal Polynomials, Mathematical problems of computer Science, No. 36, pp. 57-62, 2012.

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՎՐԱ ԱՆՎԵՐԱԾԵԼԻ ԵՎ ՆՈՐՄԱԼ ԲԱԶՄԱՆԴԱՄՆԵՐԻ ԿԱՌՈՒՑՈՒՄՆԵՐ

Ամփոփում

Մահմուդ Ալիզադեհ

Աշխատանքում ուսումնասիրվել են վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմնադամների կառուցման եղանակներ, Առաջարկվել է որոշ տեսական արդյունքների վրա հիմնաված անվերածելի բազմանդամների նորմալությունը ստուգող ալգորիթմներ, ինչպես նաև որոշ ալգորիթմներ տրված նորմալ բազմանդամի բարդությունը հաշվելու համար: Անվերածելի և նորմալ բազմանդամներն էական կիրառություն ունեն մի շարք ոլոտրներում, կոդավորման տեսություն, ծածկագրաբանություն, հաշվողական հանրահաշվական համակարգերի, գծային ռեկուրենտ հաջորդականությունների տեսություն և այլն: Անվերածելի բազմանդամները հիմնականում օգտագործվում են մեծ հզորություն ունեցող վերջավոր դաշտեր կառուցելու համար: Նորմալ բազմանդամների կիրառությունն էականորեն կապված է վերջավոր դաշտերի վրա հանրահաշվական գործողությունների բարդությունը նվազեցնելու խնդրի հետ: Ապարատային սարքերում (միկրոսխեմաներում, ԾՏԻՍ) և ծրագրային փաթեթներում վերջավոր դաշտերի վրա կատարվող գործողությունների բարդությունը որոշվում է նորմալ բազիսի ընտրությամբ: Որքան նորմալ բազմանդամի բարդությունը փոքր է, այնքան փոքր է վերջավոր դաշտերի վրա հանրահաշվական գործողությունների բարդությունը: Ստորև բերված է աշխատանքում ստացված արդյունքների համառոտ նկարագրությունը:

Թեզում ստացված հիմնական արդյունքները բերված են ստորև՝

- Տրվել է վերջավոր դաշտերի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման նոր եղանակ, որոնցում օգտագործվել է

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

տեսքի կոմպոզիցիան: Առաջարկված կոմպոզիցիաները թույլ են տալիս F_q դաշտի վրա տրված աստիճանի անվերածելի բազմանդամից կառուցել $np^k(k = 1,2,\cdots,$ pն դաշտի բնութագրիչն է) աստիճանի անվերածելի բազմանդամների հաջորդականություններ [2]:

- Տրվել է $F(x) = (x^p - x + \delta_1)^n P\left(\frac{x^p-x+\delta_0}{x^p-x+\delta_1}\right)$ տեսքի բազմանդամների վերլուծության բացահայտ տեսքը, որտեղ $P(x)$ –ը անվերածելի բազմանդամ է , և
$$F(x) = \left(\Psi\left(l(x)\right)\right)/f(x)$$
m և n աստիճանի $f(x)$ և $\bar{l}(x)$ անվերածելի բազմանդամների համար այնպես, որ $l(x)$-ը գծայնացված q-ասոցացված է $\bar{l}(x)$ բազմանդամին տրված F_q դաշտի վրա [1]:
- Տրվել է վերջավոր դաշտերի վրա նորմալ բազմանդամների բացահայտ տեսքով կառուցման նոր եղանակ, որտեղ օգտագործվել է
$$F(x) = (x^p - x + \delta)^n P\left(\frac{x^p - x}{x^p - x + \delta}\right),$$
տեսքի կոմպոզիցիան: Առաջարկված կոմպոզիցիան թույլ է տալիս F_q դաշտի վրա տրված աստիճանի նորմալ բազմանդամից կառուցել $np^k(k = 1,2\cdots,$ pն դաշտի բնութագրիչն է) աստիճանի նորմալ բազմանդամների հաջորդականություններ [3]:
- Առաջարկվել է երկու ալգորիթմ, որոնցից առաջինը թույլ է տալիս տրված F_q դաշտի վրա ստուգել տրված բազմանդամի նորմալությունը կատարելով $O(nM(n)(nlog(q) + log(n)))$ գործողություններ: Երկրորդ ալգորիթմը հնարավորություն է տալիս հաշվել տրված նորմալ բազմանդամի բարդությունը F_q դաշտում կատարելով $O\big(n(n^2 + M(n)\log(qn))\big)$ Գործողություններ: Օգտագործելով այս ալգորիթմները համեմատվել է որոշ բազմանդամների բարդությունները. Տրվել է F_p դաշտի վրա բոլոր n աստիճանի նորմալ բազմանդամները և նրանց բարդությունները ($p = 2;\ n \le 11, p = 3;\ n \le 7, p = 5;\ n \le 5, p = 7;\ n \le 4$). Ավելին, F_p դաշտի վրա մինիմալ բարդություն ունեցող բոլոր n աստիճանի նորմալ բազմանդամները բերված են [4-5]:

РЕЗЮМЕ

МАХМУД АЛИЗАДЕ

Построения непереводимых, нормальных полиномов над конечными полями

В работе рассматриваются методы построения неприводимых и нормальных многочленов на конечных полях. Предлагаются алгоритмы проверки нормальности неприводимых многочленов, основанные на некоторых теоретических результатах, а также некоторые алгоритмы для вычисления сложности заданных нормальных многочленов. Неприводимые и нормальные многочлены имеют существенное применение в ряде областей, в теории кодирования, в криптографии, в вычислительных алгебраических системах, в теории линейных рекурентных последовательностей и т.д. Неприводимые многочлены в основном используются для построения конечных полей, имеющих большую мощность. Применение нормальных многочленов существенно связано с задачей снижения сложности алгебраических действий на конечных полях. В аппаратных устройствах (микросхемах, чипах) и в программных пакетах сложность осуществляемых действий на конечных полях определяется выбором нормального базиса. Чем меньше сложность нормального многочлена, тем меньше сложность алгебраических действий на конечных полях. Ниже приведено краткое описание полученных в работе результатов.

Основные результаты, полученные в тезисе, приведены ниже:

- Дан новый метод построения неприводимых многочленов явного вида на конечных полях, в котором была использована композиция вида

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

Предложенные композиции позволяют построить последовательности неприводимых многочленов степени np^k (k =1,2,…, p - характеристика

поля) из неприводимого многочлена заданной степени на поле F_q[2].

- Дан явный вид факторизации многочленов типа

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

где $P(x)$ - неприводимый многочлен и $F(x) = (f(x))^{-1}\,\Psi\big(l(x)\big)$, Для неприводимых многочленов $f(x)$ and $\bar{l}(x)$ степени n и m, так что $l(x)$ линеаризированный многочлен q-ассоцированный с $\bar{l}(x)$ заданный на поле F_q [1].

- Дан новый метод построения нормальных многочленов явного вида на конечных полях, где использовалась композиция вида

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

Предложенная композиция позволяет построить последовательности нормальных многочленов степени np^k (k=1,2…, p – характеристика поля) из нормального многочлена заданной степени на поле F_q[3].

- Предлагаются два алгоритма, первый из которых позволяет проверить нормальность заданного многочлена на заданном поле F_q, выполнив действия $o(nM(n)(nlog(q) + \log(n)))$. Второй алгоритм дает возможность вычислить сложность заданного нормального многочлена на поле F_q, выполнив действия $O(n\big(n^2 + M(n)log(qn)\big))$. Используя эти алгоритмы, было проведено сравнение сложности некоторых многочленов: были приведены все нормальные многочлены степени n и их сложности ($p = 2; n \leq 11, p = 3; n \leq 7, p = 5; n \leq 5, p = 7; n \leq 4$) на поле F_q. Более того, все нормальные многочлены степени n, имеющие минимальную сложность на поле F_q, приводимы [4-5].

Ծավալը - 1 տ.մ. Տպաքանակը - 100 օրինակ

Տպագրված է ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային

պոլիգրաֆիայի լաբորատորիայում