ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Աբրահամյան Սերգեյ Ենոքի

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՎՐԱ ԱՆՎԵՐԱԾԵԼԻ, ՆՈՐՄԱԼ ԵՎ ՏԵՂԱԴՐՈՒԹՅԱՆ ԲԱԶՄԱՆԴԱՄՆԵՐԻ ԿԱՌՈՒՑՄԱՆ ԵՂԱՆԱԿՆԵՐ

Ա.01.09 «Մաթեմատիկական կիբեռնետիկա և մաթեմատիկական տրամաբանություն» մասնագիտությամբ ֆիզիկամաթեմատիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան 2012

ЕРЕВАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Абраамян Сергей Енокович

МЕТОДЫ ПОСТРОЕНИЯ НЕПРИВОДИМЫХ, НОРМАЛЬНЫХ И ПЕРЕСТАНОВАЧНЫХ ПОЛИНОМОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата физико-математических наук по специальности 01.01.09 “Математическая кибернетика и математическая логика”

Ереван 2012

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

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

Պաշտոնական ընդդիմախոսներ՝ ֆիզ.մաթ. գիտ. դոկտոր Լ. Հ. Ասլանյան
ֆիզ.մաթ. գիտ. թեկնածու Ժ. Գ. Մարգարյան

Առաջատար կազմակերպություն՝ Խ. Աբովյանի անվան հայկական պետական մանկավարժական համալսարան

Պաշտպանությունը կայանալու է 2012 թ. հունիսի 6-ին ժամը 14^{00}-ին ԵՊՀ-ում գործող ԲՈՀ-ի 044 «Մաթեմատիկական կիբեռնետիկա և մաթեմատիկական տրամաբանություն» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ 0025, Երևան, Ալեք Մանուկյան 1:

Ատենախոսությանը կարելի է ծանոթանալ Երևանի պետական համալսարանի գրադարանում:

Սեղմագիրն առաքվել է 2012 թ. մայիսի 5-ին:

Մասնագիտական խորհրդի գիտական քարտուղար՝
ֆիզ.մաթ. գիտ. թեկնածու Վ. Ժ. Դումանյան

Тема диссертации утверждена в институте проблем информатики и автоматизации НАН РА.

Научный руководитель: кандидат физ.-мат. наук М. К. Кюрегян

Официальные опоненты: доктор физ.-мат. наук Л. А. Асланян
кандидат физ.-мат. наук Ж. Г. Маргарян

Ведущая организация: Армянский государственный педагогический университет имени Х. Абовяна

Защита диссертации состоится 6-го июня 2012 г. В 14^{00} часов на заседании специализированного совета ВАК 044 “Математическая кибернетика и математическая логика” при ЕГУ по адресу: 0025 г. Ереван, ул. Алека Манукяна 1.

С диссертацией можно ознакомиться в библиотеке Ереванского государственного университета.

Автореферат разослан 5-го мая 2012г.

Ученый секретарь специализированного совета,
кандидат физ.-мат. наук В. Ж. Думанян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը: Վերջավոր դաշտերն սկսել են ուսումնասիրվել XIX դարի սկզբից: Այդ հասկացության ձևավորման գործում անվիճելի վաստակ են ունեցել Կառլ Գաուսը (1777 – 1855 թթ.) և Էվարիստ Գալուան (1811 – 1832 թթ.): Երկար ժամանակ վերջավոր դաշտերը հետազոտվել և կիրառություն են գտել միայն հանրահաշվում և թվերի տեսության մեջ, սակայն վերջին տասնամյակներում այդ տեսության շփումը մաթեմատիկայի տարբեր ոլորտների և նրա կիրառական բաժինների հետ զգալիորեն ընդլայնվել է: Վերջավոր դաշտերի տեսությունը հաջողությամբ համագործակցում է թվերի տեսության, խմբերի տեսության, հանրահաշվական երկրաչափության, կոմբինատորիկայի, կոդավորման տեսության և մաթեմատիկայի այլ բաժինների հետ: Վերջավոր դաշտերի տեսության բուռն վերելքին զուգընթաց զարգացում ապրեց նաև վերջավոր դաշտերի վրա սահմանված բազմանդամների տեսությունը: Վերջավոր դաշտերի վրա սահմանված բազմանդամների տեսությունը կարևոր է ոչ միայն վերջավոր դաշտերի հանրահաշվական կառուցվածքի ուսումնասիրման համար, այլև նաև ունի բազմաթիվ այլ կիրառություններ, ինչպիսիք են, օրինակ, կոդավորման տեսությունը, ծածկագրաբանությունը: Ընդ որում՝ առանձնահատուկ դեր ունեն անվերածելի, նորմալ և տեղադրության բազմանդամները, որոնք անհրաժեշտ են վերջավոր դաշտեր կառուցելու և այդ դաշտի տարրերի հետ գործողություններ կատարելու համար:

Անվերածելի բազմանդամներն էական նշանակություն ունեն մի շարք ոլորտներում՝ կոդավորման տեսություն, ծածկագրաբանություն, հաշվողական հանրահաշվական համակարգերի, գծային ռեկուրենտ հաջորդականությունների տեսություն և այլն: Ժամանակակից հաշվողական տեխնիկայի զարգացմանը զուգընթաց պահանջ է առաջանում կառուցել և ուսումնասիրել ավելի հզոր (բազմատարր) վերջավոր դաշտեր, ուստի բարձր աստիճանի անվերածելի, բազմանդամների կառուցման խնդիրը դառնում է ավելի արդիական:

Բարձր աստիճանի անվերածելի բազմանդամների կառուցման խնդրի լուծման համար գոյություն ունեն երկու սկզբունքորեն տարբեր մոտեցումներ:

Առաջին մոտեցման դեպքում տրված դաշտի վրա բոլոր հնարավոր n աստիճանի բազմանդամների բազմությունից պատահականորեն ընտրվում է մեկը: Այնուհետև հատուկ մշակված ալգորիթմի միջոցով ստուգվում է տրված դաշտի վրա այդ բազմանդամի տրոհելիությունը մի քանի այլ բազմանդամների: Եթե պարզվում է, որ հետազոտվող բազմանդամը տրոհվող է, ապա այն դեն ենք նետում և ընտրում նորը: Որոնումը շարունակվում է մինչև համապատասխան բազմանդամի գտնվելը: Նման մոտեցում առաջարկվել է Շոուպի, Ադելմանի և Լենստրայի կողմից: Երկրորդ մոտեցումը սուպերպոզիցիան է կամ կոմպոզիցիոն կառուցումը, որը հիմնված է վերջավոր դաշտերի հատկությունների և բազմանդամների անվերածելիության հատկությունների վրա: Կոմպոզիցիոն մեթոդներն առավել նախընտրելի են, քանի որ հաշվողականության տեսանկյունից ունեն փոքր բարդություն: Կոմպոզիցիոն մեթոդներով տրված ո աստիճանի անվերածելի բազմանդամների կառուցման խնդիրը մինչ օրս համարվում է վերջավոր դաշտերի տեսության չլուծված դասական խնդիրներից մեկը: Հիշատակման են արժանի Ալբերտի, Դիկսոնի, Վարշամովի, Կոհենի, Մ. Կյուրեղյանի և Գ. Կյուրեղյանի աշխատանքները:

Նորմալ բազիսների նկատմամբ աճող հետաքրքրությունը պայմանավորված է նրանց ինչպես տեսական, այնպես էլ կիրառական կարևորությամբ: Դեռ 1888 թ-ին Հենսելի կողմից նշվել էին այն առավելությունները, որոնք իհայտ են գալիս վերջավոր դաշտերը նորմալ բազմանդամների միջոցով կառուցելիս: Հարցի արծարծումը 19-րդ դարում նախանշվեց Գաուսի ուսումնասիրությամբ, որտեղ օգտագործելով նորմալ բազիսները, փորձ էր արվում միայն քանոնի և կարկինի օգնությամբ գտնել կանոնավոր բազմանկյուն կառուցելու խնդիրի լուծումը: Փաստացի, նա օգտագործում էր նորմալ բազիսները՝ ցիկլոմատիկ դաշտի ենթադաշտեր կառուցելու համար: Ի տարբերություն անվերածելի բազմանդամների՝ նորմալ բազմանդամների կիրառությունն էականորեն կապված է վերջավոր դաշտերի վրա հանրահաշվական գործողությունների բարդությունը նվազեցնելու խնդրի հետ: Ապարատային սարքերում (միկրոսխեմաներում, ՕՏԻՍ) և ծրագրային փաթեթներում վերջավոր դաշտերի վրա կատարվող գործողությունների բարդությունը որոշվում է նորմալ բազիսի ընտրությամբ: Ասվածի լավագույն ապացույց կարելի է համարել Մեսսի-Օմուրայի ալգորիթմը: Ինչպես անվերածելի բազմանդամների դեպքում, այնպես էլ նորմալ բազմանդամներ կառուցելիս նույնպես օգտագործվում են վերը նշված 2 մոտեցումները: Այս ուղղությամբ արժեքավոր

հետազոտություններ են կատարել Չապմանը Կյուրեղյանը, Լենստրան և Ջաքնիկելը:

Ոչ պակաս կարևոր են նաև տեղադրության բազմանդամները, որոնք ևս կիրառություն են գտել ծածկագրաբանության մեջ: Տեղադրության բազմանդամները սկսվել են ուսումնասիրվել դեռևս 19-րդ դարում, սակայն առաջին անգամ լուրջ ուշադրության են արժանացել Դիկսոնի և Հերմիթի աշխատանքներում: Տեղադրության բազմանդամների ուսումնասիրությունը մեծ տարածում ստացավ վերջին տասնամյակում, երբ դրանք սկսեցին լայնորեն կիրառվել ծածկագրաբանությունում: Ռ Լիդլի և Վ. Մյուլերի «PERMUTATION POLYNOMIALS IN RSA CRYPTOSYSTEM» աշխատանքում վառ արտացոլված է տեղադրության բազմանդամների կարևորությունը ծածկագրությունում:

Աշխատանքի նպատակը: Ատենախոսության հիմնական նպատակն ու խնդիրներն են.

- հետազոտել վերջավոր դաշտերի վրա տրված աստիճանի անվերածելի և նորմալ բազմանդամներից ավելի բարձր աստիճանի անվերածելի և նորմալ բազմանդամների կառուցման եղանակները, առաջարկել կոմպոզիցիոն եղանակներ բարձր աստիճանի անվերածելի և նորմալ բազմանդամների հաջորդականություններ կառուցելու համար,
- հետազոտել վերջավոր դաշտերի վրա տեղադրության բազմանդամների կառուցման եղանակները, առաջարկել տեղադրության բազմանդամների կառուցման նոր եղանակներ, կառուցել նրանց հակադարձ արտապատկերումը:

Հետազոտման օբյեկտը: Աշխատանքի հետազոտման օբյեկտը վերջավոր դաշտերի վրա սահմանված անվերածելի, նորմալ և տեղադրության բազմանդամներն են:

Հետազոտման մեթոդները: Աշխատանքում կիրառվել են թվերի տեսության, վերջավոր դաշտերի տեսության և հանրահաշվի մաթեմատիկական մեթոդներ:

Արդյունքների գիտական նորույթը: Ատենախոսությունում ստացված բոլոր արդյունքները նոր են: Ատենախոսության գիտական նորույթը որոշվում է տեսական աշխատանքների հետևյալ համախմբությամբ.

- տրվել են վերջավոր դաշտերի վրա անվերածելի բազմանդամների կառուցման կոմպոզիցիոն եղանակներ:
- Տրվել է վերջավոր դաշտերի վրա ռեկուրսիվ ձևով նորմալ բազմանդամների կառուցման կոմպոզիցիոն մի եղանակ:
- Առաջարկվել է վերջավոր դաշտերի վրա տեղադրության բազմանդամների կառուցման մի եղանակ, ինչպես նաև տրվել է $F(x) = x + \gamma f(x) + \delta g(x)$ տեսքի տեղադրության բազմանդամների հակադարձ արտապատկերման բացահայտ տեսքը:

Ստացված արդյունքների կիրառական նշանակությունը: Աշխատանքում ստացված արդյունքները կարելի է կիրառել էլեկտրոնային ստորագրության, ծածկագրաբանության, կոդավորման տեսության, ինչպես փորձարարական, այնպես էլ կիրառական ասպարեզներում, ինչպես նաև վերջավոր դաշտերի վրա անվերածելի, նորմալ և տեղադրության բազմանդամների ուսումնասիրման համար վերջավոր դաշտի էլեմենտների միջև հանրահաշվական գործողություններ կատարելիս:

Ստացված արդյունքների ապրոբացիան: Աշխատանքի հիմնական արդյունքները հրատարակված են վեց գիտական հոդվածներում: Դրանք զեկուցվել են ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի կոդավորման լաբորատորիայի ընդհանուր սեմինարում, CSIT-2011 (Հայաստան, Երևան) կոմպյուտերային գիտությանը և ինֆորմացիոն տեխնոլոգիաներին նվիրված VIII գիտաժողովում, CASC-2010 (Հայաստան, Ծաղկաձոր) և CASC-2011 (Գերմանիա, Քասել) համակարգչային հանրահաշիվ և գիտական հաշվողականությանը նվիրված միջազգային գիտաժողովներում:

Հրատարակությունները: Աշխատանքի թեմայով հրատարակվել է հինգ աշխատանք, որոնց ցուցակը բերված է սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը: Աշխատանքը բաղկացած է բովանդակությունից, ներածությունից, երեք գլուխներից, եզրակացությունից և օգտագործված գրականության ցանկից: Աշխատանքի ծավալը 79 էջ է՝ ներառյալ 36 անվանում պարունակող օգտագործված գրականության ցանկը:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածությունում հիմնավորված է թեմայի արդիականությունը, հետազոտության նպատակն ու հիմնական խնդիրները, ձևակերպված են ուսումնասիրման օբյեկտն ու հիմնադրույթները, հետազոտությունների գիտական նորույթն ու ստացված արդյունքների կիրառական նշանակությունը:

Առաջին գլխում նկարագրված են կոմպոզիցիոն մեթոդներ, որոնց օգնությամբ վերջավոր դաշտերի վրա տրված աստիճանի անվերածելի բազմանդամներից բացահայտ տեսքով կառուցվում է ավելի բարձր աստիճանի անվերածելի բազմանդամներ:

1.1 բաժնում նկարագրված է աշխատանքում օգտագործված որոշ սահմանումներ, լեմմաներ, պնդումներ և թեորեմներ:

1.2 բաժնում բերված է վերջավոր դաշտերի վրա կոմպոզիցիոն եղանակներով անվերածելի բազմանդամների կառուցման եղանակների վերաբերյալ գրականության ակնարկը:

1.3 և 1.4 բաժիններում նկարագրված են անվերածելի բազմանդամներ կառուցելու կոմպոզիցիոն եղանակները,որոնք ներկայացված են ստորև:

Դիցուք F_q -ն $q = p^s$ էլեմենտներից բաղկացած վերջավոր դաշտ է, որտեղ q-ն p պարզ թվի s աստիճանն է:

Սահմանում 1.1 Կասենք, որ $f(x) \in F_q[x]$ բազմանդամը անվերածելի է F_q դաշտի վրա (կամ $F_q[x]$ օղակում), եթե այն ունի դրական աստիճան և $f(x) = g(x) \cdot h(x)$ հավասարությունը, որտեղ $g(x), h(x) \in F_q[x]$ կարող է տեղի ունենալ միայն այն դեպքում, երբ $g(x)$-ը կամ $h(x)$-ը հաստատուն է:

Սահմանում 1.2 Դիցուք՝ տրված է $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F_q[x]$ բազմանդամը, որտեղ $a_n \neq 0$: f բազմանդամի երկակի բազմանդամ կանվանենք $f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ տեսքի բազմանդամը:

Թեորեմ 1.1 Դիցուք՝ $f(x) = x^m + a_1 x^{m-1} x + \cdots + a_m$ բազմանդամը m աստիճանի անվերածելի բազմանդամ է F_q դաշտի վրա, և $q = p^n$: Եթե $a_1 + a_1{}^p + \cdots + a_1{}^{p^{m-1}} \neq 0$, ապա

$$F(x) = \frac{1}{a_m}(1 - x^{p-1})^m f^*(\frac{x^p}{1 - x^{p-1}})$$

բազմանդամը նույնպես կլինի անվերածելի բազմանդամ F_q դաշտի վրա:

Թեորեմ 1.2 Դիցուք՝ $x^p - bx + c$ և $x^p - bx + h$ փոխադարձաբար պարզ բազմանդամներ են $F_q[x]$ օղակում և $P(x) = \sum_{i=0}^{n} c_i x^i$ բազմանդամը n աստիճանի անվերածելի բազմանդամ է F_q դաշտի վրա, և դիցուք $b \in F_q^*$ $c, h \in F_q$ $(c, h) \neq (0,0)$

Այդ դեպքում

$$F(x) = (x^P - bx + h) \; P\left(\frac{x^p - bx + c}{x^p - bx + h}\right)$$

բազմանդամը կլինի pn աստիճանի անվերածելի բազմանդամ F_q դաշտի վրա, եթե տեղի ունեն հետևյալ երկու պայմանները.

$$N_{q/p}(b) = 1 \text{ և } Tr_{q/p}\left(\frac{1}{A^p}\frac{(c-h)d_1}{c_0} + hn\right) \neq 0$$

որտեղ $A^{p-1} = b$ ինչ որ $A \in F_{q^n}$ էլեմենտի համար, իսկ

$d_1 = \sum_{i=1}^{n} i\, c_i = \frac{1}{d} P'(1)$ և $d_0 = \sum_{i=0}^{n} c_i = P(1)$:

Թեորեմ 1.3 Դիցուք՝ $P(x) = \sum_{i=0}^{n} c_i x^i$ n-աստիճանի անվերածելի բազմանդամ է F_q դաշտի վրա և դիցուք $x^p - x + \delta_1$ և $x^p - x + \delta_2$ $F_q[x]$-օղակում փոխադարձաբար պարզ բազմանդամներ են:

Սահմանենք

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

$$F_k(x) = (x^p - x + \delta_2)^{t_{k-1}} F_{k-1}\left(\frac{x^p - x + \delta_1}{x^p - x + \delta_2}\right),$$

բազմանդամների հաջորդականությունը, որտեղ $t_k = n \cdot p^k$ $F_k(x)$ բազմանդամի աստիճանն է:

Ենթադրենք $T_{r_{q/p}}\left((\delta_2-\delta_1)\frac{P'(1)}{P(1)}-\delta_2 n\right)\neq 0$ և $T_{r_{q/p}}\left(\frac{\left((\delta_1-\delta_2)P'\left(\frac{\delta_1}{\delta_2}\right)-\delta_2 nP\left(\frac{\delta_1}{\delta_2}\right)\right)}{P\left(\frac{\delta_1}{\delta_2}\right)}\right)\neq 0$

Այդ դեպքում կամայական k≥1–ի համար $F_k(x)$-բազմանդամը կլինի np^k աստիճանի անվերածելի բազմանդամ F_q դաշտի վրա:

Երկրորդ գլխում նկարագրված է մի կոմպոզիցիոն մեթոդ, որի օգնությամբ վերջավոր դաշտերի վրա տրված աստիճանի նորմալ բազմանդամներից կառուցվում է ավելի բարձր աստիճանի նորմալ բազմանդամների հաջորդականություն:

2.1 բաժնում նկարագրված է աշխատանքում օգտագործված մասնագիտական պնդումներ, սահմանումներ և թեորեմներ:

2.2 բաժնում բերված է վերջավոր դաշտերի վրա կոմպոզիցիոն եղանակներով նորմալ բազմանդամների կառուցման եղանակների վերաբերյալ գրականության ակնարկը:

2.3 բաժնում նկարագրված է նորմալ բազմանդամներ կառուցելու կոմպոզիցիոն մի եղանակ, որը ներկայացված է ստորև:

Սահմանում 2.1 F դաշտի *նորմալ բազիս* K դաշտի վրա կանվանենք $N=\{\alpha,\alpha^q,\cdots\alpha^{q^{n-1}}\}$ տեսքի այն բազիսը, որը կազմված է համապատասխան ձևով ընտրված $\alpha\in F$ էլեմենտից և նրա համալուծ էլեմենտներից:

Կասենք α-ն $N-$*նորմալ բազիսը* ծնող էլեմենտ է կամ F դաշտի *նորմալ էլեմենտ* է :

Սահմանում 2.2 $f(x)\in F_q[x]$ նորմավորված անվերծանելի բազմանդամը կանվանենք *նորմալ բազմանդամ կամ* N*-բազմանդամ*, եթե նրա արմատները կազմում են նորմալ բազիս կամ, որ համարժեք է, եթե դրանք գծորեն անկախ են F_q դաշտի վրա:

Դիցուք $n=n_1p^e$, որտեղ $p-$ն F_q դաշտի բնութագրիչն է, իսկ $GCD(p,n_1)=1$ և $e\geq 0$: Հարմարության համար նշանակենք p^e-ն $t-$ով: Ենթադրենք x^n-1 բազմանդամը վերլուծվում է $F_q[x]$ օղակում հետևյալ կերպ՝

$$x^n-1=\left(\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x)\right)^t \quad (1)$$

որտեղ $\varphi_i(x) \in F_q[x]$ իրարից տարբեր անվերածելի բազմանդամներ են, որոնք հանդիսանում են $x^n - 1$ բազմանդամի բաժանարարները:

Թեորեմ 2.1 Դիցուք $P(x) = \sum_{i=0}^{n} c_i x^i$–ը n աստիճանի անվերածելի բազմանդամ է F_q դաշտի վրա, որի երկակի բազմանդամը՝ $P^*(x)$–ը նորմալ բազմանդամ է F_q դաշտի վրա և $x^n - 1$ տրոհվում է արտադրիչների ինչպես (1)-ում :

Սահմանենք $F(x)$ բազմանդամը հետևյալ կերպ.

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

որտեղ $\delta \in F_p^*$ խմբին: Այդ դեպքում $F^*(x)$–բազմանդամը կլինի նորմալ բազմանդամ F_q դաշտի վրա, եթե տեղի ունեն հետևյալ պայմանները՝

$$Tr_{q/p}\left(\frac{P'(1)}{P(1)} - n\right) \neq 0, \qquad \frac{P'(0) + n\,P(0)}{P(0)} = \frac{c_1}{c_0} + n \neq 0,$$

որտեղ $P'(1)$–ը և $P'(0)$-ն $P(x)$ –բազմանդամի ֆորմալ ածանցյալի արժեքներն են համապատասխանաբար 1 և 0 կետերում:

Թեորեմ 2.2 Դիցուք $P(x) = \sum_{i=0}^{n} c_i x^i$ –ը n աստիճանի անվերածելի բազմանդամ է F_q դաշտի վրա, որի երկակի բազմանդամը՝ $P^*(x)$–ն նորմալ բազմանդամ է F_q դաշտի վրա, և $x^n - 1$ տրոհվում է արտադրիչների, ինչպես (1)-ում: Ռեկուրսիվ ձևով սահմանենք

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

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

բազմանդամների հաջորդականությունը, որտեղ $t_k = n \cdot p^k$-ն $F_k(x)$ բազմանդամի աստիճանն է և $\delta \in F_q^*$ խմբին: Այդ դեպքում $F_k^*(x)$ բազմանդամը կլինի նորմալ բազմանդամ F_q դաշտի վրա, եթե տեղի ունի հետևյալ պայմանները՝

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

$$Tr_{q/p}\left(\frac{P'(0) + n\,P(0)}{P(0)}\right) = Tr_{q/p}\left(\frac{c_1}{c_0} + n\right) \neq 0,$$

որտեղ $P'(1)$–ը և $P'(0)$ ն $P(x)$ բազմանդամի ֆորմալ ածանցյալի արժեքներն են 1 և 0 կետերում:

Հետևանք 2.1 Դիցուք՝ $P(x) = \sum_{i=0}^{n} c_i x^i$–ը n աստիճանի անվերածելի բազմանդամ է F_{2^s} դաշտի վրա, որի երկակի բազմանդամը՝ $P^*(x)$ –ը նորմալ բազմանդամ է F_{2^s} դաշտի վրա, և $x^n - 1$ տրոհվում է արտադրիչների ինչպես (1)ում:

Սահմանենք $F(x)$ բազմանդամը հետևյալ կերպ.

$$F(x) = \left(x^2 + x + 1\right)^n P\left(\frac{x^2 + x}{x^2 + x + 1}\right)$$

Այդ դեպքում $F^*(x)$–ը կլինի նորմալ բազմանդամ F_{2^s} դաշտի վրա, եթե տեղի ունեն հետևյալ պայմանները՝

$$Tr_{2^s/2}\left(\frac{P'(1)}{P(1)} + n\right) \neq 0 \quad \text{և} \quad \frac{c_1}{c_0} + n \neq 0,$$

որտեղ $P'(1)$–ը և $P'(0)$ ն $P(x)$ –բազմանդամի ֆորմալ ածանցյալի արժեքներն են համապատասխանաբար 1 և 0 կետերում:

Երրորդ գլխում տրվել է վերջավոր դաշտերի վրա տեղադրության բազմանդամների կառուցման մի եղանակ, ինչպես նաև $F(x) = x + \gamma f(x) + \delta\, g(x)$ տեսքի տեղադրության բազմանդամների հակադարձ արտապատկերման բացահայտ տեսքը:

3.1 բաժնում նկարագրված է տվյալ գլխում օգտագործված նեղ մասնագիտական պնդումներ, սահմանումներ և թեորեմներ:

3.2 բաժնում բերված է վերջավոր դաշտերի վրա տեղադրության բազմանդամների կառուցման եղանակների վերաբերյալ գրականության ակնարկը:

3.3 բաժնում նկարագրված է տեղադրության բազմանդամների կառուցման մի եղանակ, որը ներկայացված է ստորև:

Սահմանում 3.1 $f \in F_q[x]$ բազմանդամը կոչվում է F_q վերջավոր դաշտի տեղադրության բազմանդամ, եթե նրա հետ ասոցացված բազմանդամային ֆունկցիան $f: c \in F_q \to f(c) \in F_q$ տեղադրություն է:

Սահմանում 3.2 Կասենք, որ $\alpha \in F_{q^n}$ ոչ զրոյական էլեմենտը a գծային ձևափոխիչ է (Linear translator) $f: F_{q^n} \to F_q$ արտապատկերման համար, եթե $f(x + u\alpha) - f(x) = ua$ հավասարումը տեղի ունի կամայական $x \in F_{q^n}, u \in F_q$-ի և ամրագրված $a \in F_q$-էլեմենտի համար:

Թեորեմ 3.1 Դիցուք՝ $F(x) = x + \gamma f(x) + \delta g(x)$-ը տեղադրության բազամանդամ է F_{q^n} դաշտում որտեղ, γ և δ-ն համապատասխանաբար b_1, d_1 գծային ձևափոխիչներ են $f: F_{q^n} \to F_q$ բազմանդամի համար և b_2, d_2 գծային ձևափոխիչներ են $g: F_{q^n} \to F_q$ բազմանդամի համար: Այդ դեպքում $F(x) = x + \gamma f(x) + \delta g(x)$ տեղադրության բազմանդամի հակադարձ արտապատկերումը կլինի

$$F^{-1}(x) = x - \left(f(x) - d_1 \frac{g(x)(b_1 + 1) - b_2 f(x)}{A} \right) \frac{\gamma}{b_1 + 1} - \frac{g(x)(b_1 + 1) - b_2 f(x)}{A} \delta$$

բազմանդամը, որտեղ $A = (1 + d_2)(b_1 + 1) - d_1 b_2$:

Թեորեմ 3.2 Դիցուք՝ $\gamma, \delta, \tau, \epsilon F_{q^n}$ դաշտին և γ, δ, τ-ն համապատասխանաբար b_1, d_1, c_1 գծային ձևափոխիչներ են $f: F_{q^n} \to F_q$ բազմանդամի համար b_2, d_2, c_2 գծային ձևափոխիչներ են $g: F_{q^n} \to F_q$ բազմանդամի համար և b_3, d_3, c_3 գծային ձևափոխիչներ են $l: F_{q^n} \to F_q$ բազմանդամի համար: Այդ դեպքում

$$P(x) = x + \gamma f(x) + \delta\, g(x) + \tau l(x)$$

բազմանդամը հանդիսանում է F_{q^n} դաշտի տեղադրության բազմանդամ, եթե տեղի ունեն հետևյալ պայմանները.

- $b \neq -1$,
- $d_2 - \frac{d_1 b_2}{b_1 + 1} \neq -1$,
- $c_3 - \frac{b_3 c_1}{b_1 + 1} - \left(c_2 - \frac{b_2 c_1}{b_1 + 1} \right) \left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1 + d_2)(b_1 + 1) - d_1 b_2} \right) \neq -1$:

ՀԻՄՆԱԿԱՆ ԴՐՈՒՅԹՆԵՐՆ ՈՒ ԵԶՐԱՀԱՆԳՈՒՄՆԵՐԸ

Աշխատանքում ուսումնասիրվել են վերջավոր դաշտերի վրա անվերածելի, նորմալ և տեղադրության բազմանդամների կառուցման եղանակներ: Ստորև բերված է աշխատանքում ստացված արդյունքների համառոտ նկարագրությունը:

1. Տրվել են վերջավոր դաշտերի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման նոր եղանակներ, որոնցում օգտագործվել են $F(x) = (\ x^p - rx + h\ )^n\ P\left(\frac{x^p - bx + c}{x^p - rx + h}\right)$ և $F(x) = a_m^{-1}(1 - x^{p-1})^m f^*(\frac{x^p}{1-x^{p-1}})$ տեսքի կոմպոզիցիաները: Առաջարկված կոմպոզիցիաները թույլ են տալիս $\boldsymbol{F_q}$ վերջավոր դաշտի վրա տրված աստիճանի անվերածելի բազմանդամից կառուցել np^k $(k = 1,2\cdots$, բն դաշտի բնութագրիչն է) աստիճանի անվերածելի բազմանդամների հաջորդականությունների նոր դասեր [1][2][3]:
2. Տրվել է վերջավոր դաշտերի վրա բացահայտ տեսքով նորմալ բազմանդամների նոր դասերի կառուցման մի նոր եղանակ, որում օգտագործվել է $F(x) = (\ x^p - rx + h\ )^n\ P\left(\frac{x^p - bx + c}{x^p - rx + h}\right)$ տեսքի կոմպոզիցիան: Առաջարկված եղանակն ունի հետևյալ առավելությունները. նախապես ընտրված նորմալ բազմանդամը, ինչպես նաև վերջավոր դաշտի բնութագրիչը ֆիքսված չեն: Այսինքն կամայական վերջավոր դաշտի վրա ընտրելով n աստիճանի այնպիսի նորմալ բազմանդամ, որը բավարարում է թեորեմի պայմաններին, կարող ենք կառուցել np^k $(k = 1,2\cdots$, p դաշտի բնութագրիչն է) աստիճանի նորմալ բազմանդամների նոր դասեր [4][5]:
3. Տրվել է վերջավոր դաշտերի վրա $P(x) = x + \gamma f(x) + \delta\ g(x) + \tau l(x)$ տեսքի տեղադրության բազմանդամների կառուցման եղանակ հիմնված գծային ձևափոխիչի հատկությունների վրա, որը հնարավորություն է տալիս կառուցել տեղադրության բազմանդամների նոր դասեր, ինչպես նաև տրվել է $P(x) = x + \gamma f(x) + \delta\ g(x)$ տեսքի տեղադրության բազմանդամների հակադարձ արտապատկերումները[6]:

Ատենախոսությունում ստացված արդյունքները ունեն տեսական ու կիրառական հետաքրքրություն և կարող են կիրառվել ինչպես ծածկագրաբանության, այնպես էլ կոդավորման տեսության մեջ:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՇՐՋԱՆԱԿՆԵՐՈՒՄ ՀՐԱՏԱՐԱԿՎԱԾ ԱՇԽԱՏԱՆՔՆԵՐԻ ՑԱՆԿԸ

1. Abrahamyan S., *Construction of irreducible polynomials over finite fields*. 12th International Workshop, CASC 2010, Tsakhkadzor, Armenia, September 6-12, 2010, Proceedings. Lecture Notes in Computer Science, vol. 6244, pp. 1-4,
2. Abrahamyan S., Alizadeh M., Kyuregyan M., *Recursive constructions of irreducible polynomials over finite fields*. Finite Fields Appl. (2012), http://dx.doi.org/10.1016/j.ffa.2012.03.003 .
3. Abrahamyan S., Kyuregyan M., *A recurrent method for constructing irreducible polynomials over finite fields*. 13th International Workshop, CASC 2011, Kassel, Germany, September 5-9, 2011, Proceedings. Lecture Notes in Computer Science, vol. 6885, pp. 1-10, 2011.
4. Abrahamyan S., *Some constructions of N-polynomials over Finite Fields*. The Reports of National Academy of Sciences of Armenia, vol. 111, No 2, pp. 232-239, 2011.
5. Alizadeh M., Abrahamyan S., Saeid M., Kyureghyan M., *Constructing N-polynomials over finite fields*. Proceedings of 8th International Conference on Computer Science and Information Technologies (CSIT'2011), pp. 100-103 , 2011.
6. Abrahamyan S., Kyuregyan M., *A method of constructing permutation polynomials over finite fields*. The Reports of National Academy of Sciences of Armenia, vol. 113, No 1, pp. 51-56, 2012.

РЕЗЮМЕ

Сергей Енокович Абраамян

Метод построения непреводимых, нормальных и перестановочных полиномов над конечными полями

Данная диссертационная работа посвящена исследованию метода построения непреводимых нормальных и перестановочных полиномов над конечными полями. Известно, что эти полиномы широко используются в криптографии и теории кодирования. С развитием современных компьютерных технологий возникает необходимость построения более мощных (многоэлементных) конечных полей. Следовательно, задача построения непреводимых полиномов становится более актуальной. В настоящее время существуют два принципиально разных подхода к решению задачи построения непреводимых полиномов над конечными полями.

В случае первого подхода произвольно выбирается один полином степени n из множества всех полиномов над конечными полями. Затем, с помощью специально разработанного алгоритма проводится проверка непреводимости полинома. Поиск продолжается до тех пор, пока будет найден непреводимый полином. Второй подход – это суперпозиция или композиционный метод, основанный на свойствах конечного поля. Задача построения непреводимых полиномов с помощью метода построения является одной из сложных задач в теории конечного поля.

Применение нормальных полиномов связано с задачей изменения сложности воздействия алгебраических действий. В случае построения как непреводимых, так и нормальных полиномов используются два вышеуказанных метода. С точки зрения сложности, композиционные методы характеризуются меньшей сложностью. Задача построения нормальных полиномов с помощью метода построения является одной из сложных задач в теории конечного поля.

В последние десятилетия перестановочные полиномы получили широкое применение в области криптографии и теории кодирования. Несмотря на то, что

исследования перестановочных полиномов ведутся с XIX в., их построение считается одной из самых сложных задач в теории конечных полей.

Целью данного исследования является изучение метода построения непреводимых нормальных и перестановочных полиномов над конечными полями и предложение новых методов построения новых классов непреводимых нормальных и перестановочных полиномов над конечными полями.

Краткое описание полученных результатов дается ниже.

1. Разработаны новые методы подробного построения непреводимых полиномов, где используются композиционные методы $F(x) = (\ x^p - rx + h\ n\ Pxp{-}bx{+}c\ xp{-}rx{+}h$ и $Fx{=}am{-}1(1{-}xp{-}1)mf{*}(xp1{-}xp{-}1)$. Указанные композиционные методы позволяют построить новые классы непреводимых полиномов степени np^k ($k = 1,2\cdots$, а p является характеристикой поля) из данных полиномов степени n,[1][2][3].

2. Предложен новый метод построения нормальных полиномов, где используется композиция $F(x) = (\ x^p - rx + h\ )^n\ P\left(\frac{x^p - bx + c}{x^p - rx + h}\right)$. Преимущества предложенного метода заключаются в том, что предварительно выбранный нормальный полином и характеристика конечного поля не фиксированы. Таким образом, выбор такого нормального полинома степени n над произвольным конечным полем, который соответствует требованиям условий теоремы, дает позможность построения нового нормального полинома степени np^k ($k = 1,2\cdots$),[4][5].
3. Представлен метод построения перестановки полиномов типа $P(x) = x + \gamma f(x) + \delta\ g(x) + \tau l(x)$, который позволяет построить новые классы перестановочных полиномов, а также предложить инверсионное отображение перестановочного полинома $P(x) = x + \gamma f(x) + \delta\ g(x)$,[6].

Полученные результаты имеют как теоретическое, так и практическое значение и могут быть использованы как в области криптографии, так и в теории кодирования. Опубликовано 6 статей, материалы которых были представлены в ряде научных конференций, включая CASC2010 (Армения, Цахкадзор) , CASC2011(Германия, Кассел) и CSIT(Армения, Ереван).

A B S T R A C T

Sergey Abrahamyan

Construction methods of irreducible, normal and permutation polynomials over finite fields

The thesis deals with a study of construction methods of irreducible, normal and permutation polynomials via composition methods over finite fields. The polynomials are known to be widely used in cryptography and the coding theory. However, development of up-to-date computer technologies supports a necessity to construct stronger (poly-elemental) finite fields, this adding to topicality of a problem of construction of irreducible polynomials. Today, there exist two principally different approaches to solution of a problem of construction of irreducible polynomials over finite fields.

In the case of the first approach, one polynomial of degree n out of all polynomials of degree n over given finite field is selected arbitrary. Then through a specially developed algorithm one checks whether it is an irreducible polynomial or not. The search goes on until irreducible polynomial is identified. The second approach is a superposition or a composition method which is based on properties of the finite field. The composition methods from position of computation have lower complexity. The problem of construction of irreducible polynomials via the composition method is one of the most complex problems of a theory of finite fields.

Application of normal polynomials is associated with a problem of changing complexity of the effect of algebraic operations. In the case of construction of both irreducible and normal polynomials, the two aforesaid methods are applicable. The problem of construction of normal polynomials via the composition method is one of the most complex problems of a theory of finite fields.

In recent decades permutation polynomials gained a wide recognition in cryptograpy and coding theory. Despite a fact that permutation polynomials have been studied since XIX century, nevertheless construction of permutation polynomials is considered to be one of the most complex problems of the theory of finite fields.

The goal of this research is studying a method of construction of irreducible normal and permutation polynomials over finite fields and suggesting new methods of construction of new classes of irreducible normal and permutation polynomials over finite fields.

A brief description of the results obtained is given below.

1. Novel methods of explicit construction of irreducible polynomials are proposed, where $F(x) = (\ x^p - rx + h\ )^n\ P\left(\frac{x^p - bx + c}{x^p - rx + h}\right)$ and $F(x) = a_m^{-1}(1 - x^{p-1})^m f^*(\frac{x^p}{1-x^{p-1}})$ composition methods are used. The given composition methods enable us to construct new classes of irreducible polynomials of degree np^k ($k = 1,2\cdots$, p is a characteristic of field) from given polynomial of degree n,[1][2][3].
2. New method for explicit construction of normal polynomials is given(found), where $F(x) = (\ x^p - rx + h\ )^n\ P\left(\frac{x^p - bx + c}{x^p - rx + h}\right)$ composition method is used. The proposed method has the following advantages: Preliminary chosen normal polynomial and characteristic of finite field are not fixed. Thus, by choosing such normal polynomial of degree n over an arbitrary finite field, which agrees with our theorem's conditions, one may construct new normal polynomial of degree $np^k(k = 1,2\cdots)$,[4][5].
3. A method of constructing permutation polynomials of $P(x) = x + \gamma f(x) + \delta\ g(x) + \tau l(x)$ type is introduced. This allows to construct new classes of permutation polynomials. Additionally, introduced is the inverce mapping of the permutation polynomial $P(x) = x + \gamma f(x) + \delta\ g(x)$,[6].

The obtained results have both theoretical and applied value and can be used in both cryptography and coding theories. Some six publications were made in the frame of this research and then presented to a number of conferences including CASC2010 (Armenia, Tsaghkadzor) , CASC2011(Germany, Cassel) and CSIT(Armenia, Yerevan).