ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Էվոյան Միքայել Գագիկի

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՎՐԱ ԱՆՎԵՐԱԾԵԼԻ ԵՎ ՏԵՂԱԴՐՈՒԹՅԱՆ ԲԱԶՄԱՆԴԱՄՆԵՐԻ ԿԱՌՈՒՑՄԱՆ ԵՂԱՆԱԿՆԵՐ

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

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ 2013

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Эвоян Микаел Гагикович

МЕТОДЫ ПОСТРОЕНИЯ НЕПРИВОДИМЫХ И ПЕРЕСТАНОВОЧНЫХ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата физико-математических наук по специальности 05.13.05 “Математическое моделирование, численные методы и комплексы программ”

Ереван 2013

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

Գիտական ղեկավար՝	ֆ.մ.գ.թ.	Մ. Կ. Կյուրեղյան
Պաշտոնական ընդդիմախոսներ՝	ֆ.մ.գ.դ.	Լ. Հ. Ասլանյան
	ֆ.մ.գ.թ.	Ս. Ե. Աբրահամյան

Առաջատար կազմակերպություն՝ Երևանի պետական համալսարան

Պաշտպանությունը կայանալու է՝2013-թ. մայիսի 20-ին, ժ. 15:00-ին, 037, »Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացված պրոբլեմների ինստիտուտում (հասցեն՝ 0014, Երևան, Պ. Սևակ փ. 1):

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2013թ. ապրիլի 19-ին.

037 Մասնագիտական խորհրդի գիտական քարտուղար, ֆ.մ.գ.դ. Հ. Գ. Սարուխանյան

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	С. Е. Абраамян

Ведущая организация: Ереванский государственный университет

Защита диссертации состоится 20-го мая 2013 г. В 15:00 часов на заседании специализированного совета N 037 “Математическое моделирование, численные методы и комплексы программ” при Институте проблем информатики и автоматизации НАН РА по адресу: 0014 г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке института.
Автореферат разослан 19-го апреля 2013г.

Ученый секретарь специализированного совета 037, доктор физ.-мат. наук А. Г. Саруханян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը: Աշխատանքը նվիրված է վերջավոր դաշտերի վրա անվերածելի և տեղադրության բազմանդամների ուսումնասիրությանը: Հայտնի է, որ վերջավոր դաշտերի տեսությունը շատ կիրառություններ ունի ժամանակակից դիսկրետ մաթեմատիկայում, որոնցից են կոդավորման տեսությունը (տես Ռ.Լիդլի և Նիդեռայեռի «Finite Fields» գրքի 9.1 և 9.2 բաժիններ), և ծածկագրաբանությունը: Այն օգտագործվում է նաև պսեվդո-պատահական թվեր գեներացնելու համար, և որոշակի կոմբինատոր օբյեկտներ կառուցելում համար (տես Ռ. Լիդլին Գ. Պիլցի “Applied abstract algebra” գրքի 5.1 բաժնում): Ժամանակակից համակարգչային տեխնոլոգիաների զարգացմանը զուգընթաց անհրաժեշտություն առաջացավ ավելի հզոր (բազմատարր) վերջավոր դաշտեր կառուցել: Իսկ այդպիսի դաշտերի կառուցման հիմնական եղանակն է վերջավոր դաշտերի ընդլայնումը անվերածելի բազմանդամների միջոցով:

Ներկայումս վերջավոր դաշտերի վրա անվերածելի բազմանդմների կառուցման խնդիրը լուծելու երկու սկզբունքորեն տարբեր մոտեցումներ կան: Առաջին մոտեցման դեպքում դաշտի վրա բոլոր հնարավոր տրված n աստիճանի բազմանդամների բազմությունից պատահականորեն ընտրվում է մեկը: Այնուհետև հատուկ մշակված ալգորիթմի միջոցով ստուգվում է այդ բազմանդամի տրոհելիությունը մի քանի այլ բազմանդամների տրված դաշտի վրա: Եթե պարզվում է, որ հետազոտվող բազմանդամը տրոհվող է, ապա այն դեն ենք նետում և ընտրում նորը: Որոնումը շարունակվում է այնքան, մինչև համապատասխան բազմանդամի գտնվելը: Նման մոտեցումներից է Վ. Շոուպի առաջարկած մեթոդը: Այս մեթոդի թերություններից է բարձր աստիճանի անվերածելի բազմանդամների կառուցման համար մեծ հաշվողական հզորությունների պահանջը: Երկրորդ մոտեցումը սուպերպոզիցիան է կամ կոմպոզիցիոն կառուցումը, որը հիմնված է վերջավոր դաշտերի հատկությունների և բազմանդամների անվերածելիության հատկությունների վրա: Կոնստրուկտիվ մեթոդները օգտակար են նաև հաշվողական տեսանկյունից, քանի որունեն ավելի փոքր բարդություն: Կոմպոզիցիոն մեթոդներով տրված n աստիճանի անվերածելի բազմանդամների կառուցման խնդիրը F_q դաշտի վրա մինչ օրս համարվում է վերջավոր դաշտերի տեսության չլուծված դասական խնդրիներից մեկը: Այս ուղղությամբ հիշատակման են արժանի Ա. Ալբերտի, Է. Դիկսոնի, Ռ.Վարշամովի, Ս. Կոհենի և Մ. Կյուրեղյանի աշխատանքները:

Մեծ կարևորություն ունեն են նաև վերջավոր դաշտերի վրա սահմանված տեղադրության բազմանդամները, որոնք ևս կարևոր կիրառություն են գտել ծածկագրաբանության և կոդավորման տեսության մեջ: Տեղադրության բազմանդամները առաջին անգամ լուրջ ուշադրության են արժանացել Է. Դիկսոնի

աշխատանքում: Վերջերս հետաքրքրություն աճ է նկատվում F_q վերջավոր դաշտերի ոչ տրիվիալ տեղադրությանբազմանդամների կառուցման խնդրի նկատմամբ, ինչը պայմանավորված է այդ բազմանդամների կիրառություններով կոդավորման տեսությունում, ծածկագրաբանություն և կոմբինատորիկայում: Այն, որ տեղադրության բազմանդամները օգտագործվում են ծածկագրահամակարգերում, զարմանալի չէ, քանի որ նրանց կարելի է օգտագործել այբուբենը տեղաշարժման միջոցով ծածկագրելու համար: Տեղադրության բազմանդամները նաև օգտագործվում են սխալներ գտնող և ուղղող ալգորիթմներում: Ռ.Լիդլի և Վ. Մյուլերի «PERMUTATION POLYNOMIALS IN RSA CRYPTOSYSTEM» աշխատանքում վառ արտացոլված է տեղադրության բազմանդամների կարևորությունը ծածկագրաբանությունում: Տեղադրության բազմանդամների օգտագործման օրինակներից է իրենց օգտագործումը **LDPC**(Low-density parity-check) կոդերի կառուցումում: Այս ուղղությամբ հիշատակման են արժանի Ռ.Լիդլի, Վ. Մյուլերի, Օ.Տակեշիտայի, Գ.Կյուրեղյանի և Պ.Չապինի աշխատանքները:

Աշխատանքի նպատակը: Ատենախոսության հիմնական նպատակներն են

- Հետազոտել վերջավոր դաշտերի վրա տրված աստիճանի անվերածելի բազմանդամներից ավելի բարձր աստիճանի անվերածելի բազմանդամների կառուցման եղանակները:
    1. Առաջարկել բարձր աստիճանի անվերածելի բազմանդամների և անվերածելի բազմանդամների հաջորդականություններ կառուցելու նոր եղանակներ:
    2. Առաջարկել պրիմիտիվ և նորմալ բազմանդամների կառուցման նոր եղանակներ:
- Հետազոտել վերջավոր դաշտերի տեղադրության բազմանդամների կառուցման եղանակները:
    1. Առաջարկել վերջավոր դաշտերի վրա գծային ձևափոխիչների օգնությամբ տեղադրության բազմանդամների կառուցման եղանակներ:
    2. Հետազոտել բազմանդամների մի դաս F_{q^2} դաշտի վրա և տալ նրանց տեղադրության բազմանդամ լինելու հայտանիշներ:

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

Հետազոտման մեթոդները: Աշխատանքում օգտագործված են թվերի տեսության, վերջավոր դաշտերի տեսության, հանրահաշվական կոդավորման տեսության և հանրահաշվի մեթոդներ:

Արդյունքների գիտական նորույթը: Ատենախոսությունում ստացված արդյունքների գիտական նորույթը որոշվում է տեսական աշխատանքների հետևյալ համախմբությամբ.

- Առաջարկվել են կոնստրուկտիվ մեթոդներ, որոնց օգնությամբ հնարավոր է կառուցել բարձր աստիճանի անվերածելի բազմանդամներ և անվերածելի բազմանդամների հաջորդականություններ: Առաջարկվել է նաև վերջավոր դաշտերի վրա պրիմիտիվ բազմանդամներից նույն աստիճանի պրիմիտիվ բազմանդամների կառուցման կոնստրուկտիվ մեթոդ: Հետազոտվել է բազմանդամների մի դասի տրոհելիությունը:
- Սահմանվել է k-փոխանակումը և ներկայացվել են նրա հատկություններ: Առաջարկվել է վերջավոր դաշտերի վրա տեղադրության բազմանդամների և նրանց հակադարձ բազմանդամների կառուցման նոր եղանակ, որում օգտագործվում են գծային ձևափոխիչները և k-փոխանակումները: Ինչպես նաև հետազոտվել է F_{q^2} դաշտի վրա բազմանդամների մի դաս և ընդհանրացվել է Ակլբարիի արդյունքներից մեկը:

Ստացված արդյունքների կիրառական նշանակությունը: Աշխատանքում ստացված արդյունքները կարելի է կիրառել էլեկտրոնային ստորագրության, ծածկագրաբանության, կոդավորման տեսության, ինչպես փորձագիտական այնպես էլ կիրառական ասպարեզներում, ինչպես նաև վերջավոր դաշտերի վրա անվերածելի 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-րդ գիտաժողովում, CSIT-2009 (Հայաստան, Երևան) կոմպյուտերային գիտությանը և ինֆորմացիոն տեխնոլոգիաներին նվիրված VII-րդ գիտաժողովում, CSIT-2007 (Հայաստան, Երևան) կոմպյուտերային գիտությանը և ինֆորմացիոն տեխնոլոգիաներին նվիրված VI-րդ գիտաժողովում: Այս թեզի նյութերի արդյունքներին նվիրված վեց գիտական հոդվածներ են տպագրվել է:

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

Ատենախոսության կառուցվածքը և ծավալը: Աշխատանքը բաղկացած է բովանդակությունից, ներածությունից, երեք գլուխներից, եզրակացությունից և օգտագործված գրականության ցանկից: Աշխատանքի ծավալն է 101 էջ՝ ներառյալ 47 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 մեթոդներ, որոնց օգնությամբ վերջավոր դաշտերի վրա տրված աստիճանի անվերածելի բազմանդամներից բացահայտ տեսքով կառուցվում են անվերածելի բազմանդամների հաջորդականություններ: Ինչպես նաև տրվում են տրված աստիճանի անվերածելի բազմանդամներից բացահայտ տեսքով ավելի բարձր աստիճանի անվերածելի բազմանդամների կառուցման մեթոդներ: Նաև հետազոտվում է բազմանդամների մի դասի տրոհելիությունը:

1.1 բաժնում նկարագրված են 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 բաժնում ներկայացված են վերջավոր դաշտերի վրա անվերածելի, նորմալ և պրիմիտիվ բազմանդամների կառուցման էֆֆեկտիվ մեթոդներ:Այս գլխում տրված են բազմանդամների որոշակի դասի արտադրիչների տրոհման մասին արդյունքներ:

1.4 բաժնում նկարագրված են Դիկսոնի և Սիդելնիկովի արդյունքների վրա հիմնված $n(q^n-1)$ և $n(q^n+1)$ աստիճանի անվերածելի բազմանդամներ կառուցելու կոմպոզիցիոն եղանակները:

1.5 բաժնում ներկայացված են F_p դաշտի վրա pt աստիճանի անվերածելի բազմանդամների կառուցման էֆֆեկտիվ մեթոդներ F_p-ում պրիմիտիվ

էլեմենտների միջոցով: Այս բաժնում նաև տրված են Վարշամովի կողմից առանց ապացույցի տպագրված մի արդյունքի ապացույց:

Սահմանում 1.1 Դիցուք R որևէ օղակ է: Եթե գոյություն ունի այնպիսի բնական n թիվ, որ կամայական $r \in R$-ի համար տեղի ունի $nr = 0$ հավասարությունը, ապա այդպիսի ամենափոքր թիվը կոչվում է R օղակի բնութագրիչ, իսկ R կոչվում է n բնութագրիչով օղակ: Եթե այդպիսի n բնական թիվ գոյություն չունի, ապա R կանվանենք 0 բնութագրիչով օղակ:

Սահմանում 1.2 R օղակի վրա $n \geq 0$ աստիճանի բազմանդամ կանվանենք $f(x) = a_0 + a_1x + \cdots + a_nx^n$ տեսքի արտահայտությունը, որտեղ a_i գործակիցները R օղակի էլեմենտներ են և $a_n \neq 0$

Սահմանում 1.3 $f \in F_q[x]$ բազմանդամը կոչվում է անվերածելի բազմանդամ F_q դաշտի վրա, եթե այն ունի դրական աստիճան և $f(x) = g(x) \cdot h(x)$ հավասարությունը, որտեղ $g, h \in F_q[x]$, տեղի ունի միայն այն դեպքում, երբ $g(x)$-ը կամ $h(x)$-ը հաստատուն են:

Սահմանում 1.4 Դիցուք $K = F_q$, $F = F_{q^m}$ և $\alpha \in F$: Սահմանենք α էլեմենտի հետք K դաշտի վրա հետևյալ կերպ.

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}:$$

Եթե K-ն F դաշտի պարզ ենթադաշտ է, ապա $Tr_{F/K}(\alpha)$ կոչվում է α էլեմենտի բացարձակ հետք և նշանակվում է $Tr_F(\alpha)$:

Թեորեմ 1.1 Դիցուք $P(x) = \sum_{u=0}^{n} a_u x^u \in F_q[x]$-ը $n \geq 2$ աստիճանի անվերածելի բազմանդամ է, որտեղ գոնե մեկ գործակից $a_{2i+1} \neq 0$ $\left(0 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor\right)$ և $P(x)$ կարգը հավասար է e-ի: Այդ դեպքում

$$g_P(x) = (-1)^n \sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^u a_u a_{2j-u} x^j$$

բազմանդամը կլինի n աստիճանի անվերածելի բազմանդամ F_q դաշտի վրա, և կունենա $\frac{e}{GCD(e,2)}$ կարգ: Ավելին $g_p(x)$-ը կհանդիսանա α^2 մինիմալ բազմանդամը, որտեղ α և հանդիսանում է $P(x)$ արմատ:

Հետևանք 1.1 Դիցուք $q = p^s$, որտեղ p-ն կենտ պարզ թիվ է, δ-ն F_q-ի կամայական պրիմիտիվ էլեմենտ է և $P(x) = \sum_{u=0}^{n} a_u x^u \in F_q[x]$-ը կենտ n աստիճանի պրիմիտիվ բազմանդամ է: Ապա

$$\delta^n g_P\left(\frac{x}{\delta}\right) = \sum_{j=0}^{n}\sum_{u=0}^{2j}(-1)^{u+1}a_u a_{2j-u}x^j\delta^{n-j}$$

բազմանդամը n աստիճանի պրիմիտիվ բազմանդամ է F_q-ի վրա:

Թեորեմ 1.2 Դիցուք $p > 2$ պարզ թիվ է, α-ն F_p-ի կամայական պրիմիտիվ էլեմենտ է, և t բնական թիվը այնպիսին է, որ իր բոլոր պարզ բաժանարարները նաև $(p-1)$-ի բաժանարարներ են: Ենթադրենք նաև որ $t \not\equiv 0(mod\ 4)$ եթե $p^p \equiv -1(mod\ 4)$: Ապա

$$f_t(x) = \sum_{u=0}^{p-1}\alpha^u x^{(p-u)t} - \alpha$$

բազմանդամը pt աստիճանի և et կարգի անվերածելի բազմանդամ է F_p-ում, որտեղ e-ն $f_1(x)$ կարգն է:

Հետևանք 1.2 Դիցուք $p > 2$ պարզ թիվ է, α-ն F_p-ի կամայական պրիմիտիվ էլեմենտ է: Ապա

$$f(x) = \sum_{u=0}^{p-1}\alpha^u x^{(p-u)} - \alpha$$

բազմանդամը նորմալ բազմանդամ է F_p-ի վրա:

Թեորեմ 1.3 Դիցուք $q = p^s$, որտեղ p-ն պարզ թիվ է, $P(x) = \sum_{u=0}^{n} a_u x^u$ F_q-ի վրա n աստիճանի անվերածելի բազմանդամ է, $P(x)$ բազմանդամի կարգը հավասար է և t-ն այնպիսին է, որ իր բոլոր պարզ բաժանարարները նաև e-ի բաժանարարներ են, բայց չեն բաժանում $(q^n-1)e^{-1}$ թիվը: Ենթադրենք, որ $t \equiv 0(mod\ 4)$ եթե $q^n \equiv 1(mod\ 4)$: Եթե $Tr_{F_{p^s}/F_p}(a_{n-1}) \neq 0$, ապա ntp աստիճանի

$$P(x^{pt} - x^t)$$

բազմանդամը անվերածելի է F_q-ում և նրա կարգը հավասար է ht, որտեղ h-ը $P(x^p - x)$ բազմանդամի կարգն է:

Թեորեմ 1.4 Դիցուք $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 n$ աստիճանի անվերածելի բազմանդամ է $F_q = F_{p^s}$-ում: Ենթադրենք $\delta_0 \in F_p$, $g(\delta_0) \in F_p^*$ և $Tr_{F_q/F_p}(n\delta_0 + a_{n-1}) = 0$: Սահմանենք

$$f_0(x) = g(x^p - x + \delta_0),$$
$$f_k(x) = f_{k-1}^*(x^p - x + \delta_k),$$

որտեղ $k \geq 0$ և $\delta_1, \dots, \delta_k \in F_p$: Ենթադրենք նաև, որ f_0^* ունի ճիշտ t արտադրիչ՝ $v_i(x), i = 1, \dots, t$, որոնց x^{n-1}-ի գործակիցները (նշանակենք դրանց $a_{n-1}^{(i)}, i = 1, \dots, t$) բավարարում են

$$Tr_{F_q/F_p}\left(n\delta_1 + a_{n-1}^i\right) Tr_{F_q/F_p}\left(v_i'(\delta_1)\right) \neq 0,$$

ապա f_k-ն ունի ճիշտ t քանակությամբ np^k աստիճանի անվերածելի արտադրիչ, իսկ f_k բազմանդամի մյուս անվերածելի արտադրիչները np^u տեսքի են, որտեղ $u < k$: Ընդ որում f_k-ը տրոհվում է $F_{q^{np^k}}$-ի վրա: Ավելին, եթե $t \geq 1$, ապա այն դաշտը, որի վրա f_k-ի տրոհվում է, $F_{q^{np^k}}$ դաշտն է:

Թեորեմ 1.5 Դիցուք $q^n > 2$, $f(x) \neq x - 1$ բազմանդամը n աստիճանի պրիմիտիվ բազմանդամ է F_q-ի վրա, $\beta, \gamma \in F_q, \beta \neq \pm\gamma$ և

$$h(x) = f\big((\beta + \gamma)x + 1\big):$$

Ապա $n(q^n - 1)$աստիճանի

$$F(x) = (x - \gamma)^n \, f((x - \gamma)^{-1}(x^{q^n} + \beta)) \times (h^*(x - \gamma))^{-1}$$

բազմանդամը F_q-ի վրա անվերածելի է:

Թեորեմ 1.6 Դիցուք $f(x)$-ը $2n$ աստիճանի և $e(q^n + 1)$ կարգի անվերածելի բազմանդամ է F_q-ի վրա, $x^{eq^n} + x^e + 1 \equiv R(x)(mod\, f(x))$ և $\Psi(x) = \sum_{v=0}^{n} \Psi_u x^u$, որտեղ ամենափոքր աստիճանի ոչ 0-ական բազմանդամ է, որը բավարարում է

$$\sum_{v=0}^{n} \Psi_u (R(x))^u \equiv 0\big(mod\, f(x)\big):$$

Ապաn աստիճանի $\Psi(x)$ և $n(q^n + 1)$ աստիճանի

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

բազմանդամները անվերածելի բազմանդամներ են F_q-ի վրա:

Թեորեմ 1.7 Դիցուք $p > 2$ պարզ թիվ է, α-ն F_p-ի կամայական պրիմիտիվ էլեմենտ է, β-ն F_p-ի կամայական էլեմենտ է: Ապա

$$F(x) = \sum_{u=0}^{p-1} (ax - \beta)^u x^{(p-1-u)p} - \alpha$$

բազմանդամը $p(p - 1)$ աստիճանի անվերածելի բազմանդամ է F_p դաշտի վրա:

Աշխատանքում ներկայացվել են նաև թեորեմներ 1.1, 1.2 և 1.3 վրա հիմնված ալգորիթմները:

Երկրորդ գլխում նկարագրված են վերջավոր դաշտերի վրա արտապատկերումների k-փոխարկումները և նրանց հատկությունները: Ինչպես նաև հետազոտվել են $f_{a,b,\alpha,k}(x) = ax^q + bx + \alpha(x^q + x)^k$ տեսքի բազմանդամները F_{q^2} դաշտի վրա:

2.1 բաժնում նկարագրված են սույն գլխում օգտագործված որոշ սահմանումներ, լեմմաներ, պնդումներ և թեորեմներ:

2.2 բաժնում բերված է վերջավոր դաշտերի վրա տեղադրությունների մի դասի տեղադրության բազմանդամ լինելուն արդյունքներ:

2.3 բաժնում հետազոտվել են $f_{a,b,\alpha,k}(x) = ax^q + bx + \alpha(x^q + x)^k$ տեսքի բազմանդամները F_{q^2} դաշտի վրա, և տրվել են նրանց տեղափոխության բազմանդամ լինելու երկու հայտանիշ:

2.4 բաժնում նկարագրված են վերջավոր դաշտերի վրա արտապատկերումների k-փոխարկումները, նրանց հատկությունները և $F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x)$ տեսքի տեղադրության բազմանդամների կառուցման եղանակ k-փոխարկումները միջոցով, որը հնարավորություն է տալիս կառուցել տեղադրության բազմանդամների նոր դասեր, ինչպես նաև այդ տեղադրության բազմանդամների հակադարձ արտապատկերումները բացահայտ տեսքով:

Սահմանում 2.1 $f \in F_q[x]$ բազմանդամը կոչվում է F_q վերջավոր դաշտի տեղադրության բազմանդամ, եթե նրա հետ ասոցացված բազմանդամային ֆունկցիան $f: c \in F_q \to f(c) \in F_q$ հանդիսանում է տեղադրություն: Ակնհայտ է, որ եթե F_q դաշտում f-ը հանդիսանում է տեղադրության բազմանդամ ապա $f(x) = a$ հավասարումը ունի ճիշտ մեկ լուծում F_q-դաշտում յուրաքանչյուր $a \in F_q$-էլեմենտի համար:

Սահմանում 2.2 Կասենք որ $\alpha \in F_{q^n}$ ոչ զրոյական էլեմենտը a գծային ձևափոխիչ է $f: F_{q^n} \to F_q$ 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 ֆիքսված $a \in F_q$-ի համար:

Սահմանում 2.3 Դիցուք $F: F_{q^n} \to F_{q^n}$ և $(\gamma_1, \gamma_2, \dots, \gamma_n)$-ը F_{q^n}-ի բազիսն է F_q-ի նկատմամբ: Ապա միարժեք որոշված $f_i: F_{q^n} \to F_{q^n}, 1 \le i \le n$ ֆունկցիաները, որոնց համար ճիշտ է

$$F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x),$$

կանվանենք $F(\mathrm{x})$-ի կոորդինատային ֆունկցիաներ $(\gamma_1, \gamma_2, \dots, \gamma_n)$ բազիսի նկատմամբ:

Սահմանում 2.4 Դիցուք $F: F_{q^n} \to F_{q^n}$: $F(\mathrm{x})$-ի կոմպոնենտային ֆունկցիաներ F_q-ի նկատմամբ կանվանենք $Tr_{q^n}/_q\big(\alpha F(x)\big)$, որտեղ $\alpha \in F_{q^n}^*$:

Սահմանում 2.5 $F: F_{q^n} \to F_{q^n}$ արտապատկերումը կանվանենք $G: F_{q^n} \to F_{q^n}$ փոխանակում, եթե գոյություն ունի F_{q^n}-ի F_q-ի նկատմամբ $(\gamma_1, \gamma_2, \dots, \gamma_n)$ այնպիսի բազիս, որ

$$F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x),$$

և

$$G(\mathrm{x}) = \gamma_1 g_1(x) + \gamma_2 g_2(x) + \cdots + \gamma_n g(x),$$

որտեղ $f_1(x) \neq g_1(x)$ և $f_i(x) = g_i(x)$ երբ $2 \leq i \leq n$:

Սահմանում 2.6 Դիցուք $1 \leq k \leq n$: $F: F_{q^n} \to F_{q^n}$ արտապատկերումը կանվանենք $G: F_{q^n} \to F_{q^n}$-ի k-փոխանակում, եթե k-ն փոքրագույն բնական թիվն է, որի համար գոյություն ունի F_{q^n}-ի F_q-ի նկատմամբ$(\gamma_1, \gamma_2, \dots, \gamma_n)$ այնպիսի բազիս, որ

$$F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x),$$

և

$$G(\mathrm{x}) = \gamma_1 g_1(x) + \gamma_2 g_2(x) + \cdots + \gamma_n g_n(x),$$

որտեղ $f_j(x) \neq g_j(x)$ երբ $1 \leq j \leq k+1$ և $f_i(x) = g_i(x)$ երբ $k+1 \leq i \leq n$:

Թեորեմ 2.1 Դիցուք $q = p^m$ և $f_{a,b,\alpha,k}(x) \coloneqq ax^q + bx + \alpha(x^q + x)^k$, որտեղ $a, b, \alpha \in F_{q^2}$ այնպիսին են, որ $\left(\frac{b}{a}\right)^{q+1} \neq 1$ կամ $b \neq 0$ և $a = 0$: Ապա $f_{a,b,\alpha,k}(x)$ տեղադրության բազմանդամ է F_{q^2} դաշտի վրա այն և միայն այն դեպքում, երբ $g(x) = x + (\gamma^q + \gamma)x^k$ հանդիսանում է F_q դաշտի վրա տեղադրության բազմանդամ, որտեղ $\alpha = a\gamma^q + b\gamma$:

Թեորեմ 2.2 Դիցուք $q = p^m$ և $f_{a,b,\alpha,k}(x) \coloneqq ax^q + bx + \alpha(x^q + x)^k$,որտեղ $a, b, \alpha \in F_{q^2}$, $\left(\frac{b}{a}\right)^{q+1} = 1$ և $gcd(k, q-1) = 1$: Ապա $f_{a,b,\alpha,k}(x)$ տեղադրության բազմանդամ է F_{q^2} դաշտի վրաայն և միայն այն դեպքում, երբ $a \neq b$ և $\gamma \notin Image(L)$:

Թեորեմ 2.3 Դիցուք $1 \leq k \leq n$ և $F, G: F_{q^n} \to F_{q^n}$: Ապա հետևյալ պնդումները համարժեք են

(i) F-ը G-ի k-փոխանակում է:

(ii) $F - G: x \to F(x) - G(x)$-ի արտապատկերման պատկերներ բազմությունը ծնում է k-չափանի վեկտորական տարածություն F_q-ի նկատմամբ:

Թեորեմ 2.4 Դիցուք $1 \leq k \leq n, \lambda_1, \lambda_2, \dots, \lambda_k \in F_{q^n}$-ները գծորեն անկախ են F_q-ի վրա և $f_i: F_{q^n} \to F_q$, $i = 1, \dots, k$: Ավելին, ենթադրենք λ_i-ն f_j–ի $b_{j,i}$գծային ձևափոխիչ է, որտեղ $i, j \in \{1,2, \dots, k\}$: Նշանակենք

$$B \coloneqq \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \dots & b_{1,k} \\ b_{2,1} & 1+b_{2,2} & \dots & b_{2,k} \\ & & \ddots & \\ b_{k,1} & b_{k,2} & \dots & 1+b_{k,k} \end{pmatrix}$$

և սահմանենք և $F: F_{q^n} \to F_{q^n}$-ը $F(\mathrm{x}) = x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_k f_k(x)$:

Ապա $F(x) = F(y)$, որտեղ $x, y \in F_{q^n}$, այն և միայն այն դեպքում, երբ $y = x + \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_k a_k$, որտեղ $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} \in F_{q^n}$ պատկանում է B-ի միջուկին: Մասնավորապես, F արտապատկերումը q^{n-r}-ից 1 արտապատկերում է F_{q^n}-ում, որտեղ r-ը B մատրիցի ռանգն է:

Հետևանք 2.1 Դիցուք $1 \le k \le n$, $\lambda_1, \lambda_2, \dots, \lambda_k \in F_{q^n}$-ները գծորեն անկախ են F_q-ի վրա և $f_i: F_{q^n} \to F_q, i = 1, \dots, k$: Ավելին, ենթադրենք λ_i-ն f_j–ի $b_{j,i}$գծային ձևափոխիչ է, որտեղ $i, j \in \{1,2, \dots, k\}$: Նշանակենք

$$B \coloneqq \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \dots & b_{1,k} \\ b_{2,1} & 1+b_{2,2} & \dots & b_{2,k} \\ & & \ddots & \\ b_{k,1} & b_{k,2} & \dots & 1+b_{k,k} \end{pmatrix}$$

Նաև սահմանենք $F: F_{q^n} \to F_{q^n}$-ը՝ $F(\mathrm{x}) = x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_k f_k(x)$:Ապա $F(\mathrm{x})$ կլինի փոխմիարժեք այն և միայն այն դեպքում, երբ B-ի ռանգը k է: Ենթադրենք B^{-1}-ը B-ի հակադարձ մատրիցն է: Եթե նշանակենք $h_j: F_{q^n} \to F_q$, $j = 1, \dots, k$

$$\begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_j(x) \end{pmatrix} \coloneqq B^{-1} \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_k(x) \end{pmatrix}$$

ապա $F(\mathrm{x})$ բազմանդամի հակադարձ մատրիցը կտրվի

$$F^{-1}(x) = x - \sum_{j=1}^{k} \lambda_j h_j(x)$$

բանաձևով:

Երրորդ գլխում նկարագրված են նախորդ գլուխներում ստացված արդյունքների կիրառություններ:

3.1 բաժնում նկարագրված են սույն աշխատանքումստացված արդյունքների կիրառությունը ցիկլիկ կոդերի կառուցման մեջ:

3.2 բաժնում նկարագրված են սույն աշխատանքումստացված արդյունքների կիրառությունը Գոպպայի կոդերի կառուցման մեջ:

ՀԻՄՆԱԿԱՆ ԴՐՈՒՅԹՆԵՐՆ ՈՒ ԵԶՐԱՀԱՆԳՈՒՄՆԵՐԸ

Աշխատանքը նվիրված է վերջավոր դաշտերի վրա անվերածելի և տեղադրության բազմանդամների կառուցման եղանակներին: Ստորև բերված են աշխատանքում ստացված արդյունքների համառոտ նկարագրությունը:

1. Տրվել են վերջավոր դաշտերի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման նոր եղանակներ: Առաջարկվել են et աստիճանի

$$f_t(x) = \sum_{u=0}^{p-1} \alpha^u x^{(p-u)t} - \alpha$$

տեսքի, $p(p-1)$ աստիճանի

$$\sum_{u=0}^{p-1} (ax-\beta)^u x^{(p-1-u)p} - \alpha$$

տեսքի և ntp աստիճանի $P(x^{pt}-x^t)$ տեսքի անվերածելի բազմանդամների կառուցման մեթոդներ: Առաջարկված է $P(x)=\sum_{u=0}^{n} a_u x^u$ տեսքի անվերածելի բազմանդամից նույն աստիճանի անվերածելի բազմանդամների կառուցման մեթոդ, որում համար օգտագործվել է

$$g_P(x) = \sum_{\substack{0\le j\le n \\ u+v=2j, v<u\le n}} ((-1)^u 2a_u a_v + (-1)^j a_j^2)x^j$$

տեսքի բազմանդամը: Ինչպես տրված են պրիմիտիվ $P(x)=\sum_{u=0}^{n} a_u x^u$ բազմանդամից

$$\sum_{j=0}^{n}\sum_{u=0}^{2j} (-1)^{u+1} a_u a_{2j-u} x^j \delta^{n-j}$$

տեսքի F_q պրիմիտիվ բազմանդամների կառուցման եղանակներ, [1, 2, 3]:

2. Տրվել են վերջավոր դաշտերի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման նոր եղանակներ, որոնցում օգտագործվել են

$(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta)) \times \left(h^*(x-\gamma)\right)^{-1}$ և $F(x) = x^n \Psi\left(\frac{x^{q^n+1}+x^{q^n}+1}{x}\right)$

տեսքի կոմպոզիցիաները: Առաջարկված կոմպոզիցիաները թույլ են $n(q^n-1)$

և $n(q^n+1)$ աստիճանի անվերածելի բազմանդամներ կառուցել F_q դաշտի վրա, [4]:

3. Նկարագրվել և հետազոտվել են վերջավոր դաշտերի վրա արտապատկերումների k-փոխարկումները և նրանց հատկությունները: Տրվել է վերջավոր դաշտերի վրա $F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x)$ տեսքի տեղադրության բազմանդամների կառուցման եղանակ, որը հնարավորություն է տալիս կառուցել տեղադրության բազմանդամների նոր դասեր, ինչպես նաև այդ տեղադրության բազմանդամների հակադարձ արտապատկերումները բացահայտ տեսքով: Ինչպես նաև հետազոտվել են $f_{a,b,\alpha,k}(x) = ax^q + bx + \alpha(x^q + x)^k$ տեսքի բազմանդամները F_{q^2} դաշտի վրա, և տրվել են նրանց տեղափոխության բազմանդամ լինելու երկու հայտանիշներ, [5, 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] M. K. Kyuregyan and M. G. Evoyan, "Explicit Construction Theorems on Generator Polynomials," *Proceedings of 6th International Conference on Computer Science and Information Technologies (CSIT'2007),* p. 111, 2007.

[2] M. K. Kyuregyan, E. Y. Harutyunyan and M. G. Evoyan, "On a Class of Irreducible Polynomials Over F_p," *Mathematical Problems Of Computer Science,* vol. XXXI, pp. 5-15, 2008.

[3] M. K. Kyuregyan and M. G. Evoyan, "On Constructing Irreducible Polynomials over Finite Fields based on Polynomial Composition and The Reducibility of Some Polynomials over Finite Fields," *Proceedings of 8th International Conference on Computer Science and Information Technologies (CSIT'2011),* pp. 114-116, 2011.

[4] M. K. Kyuregyan and M. G. Evoyan, "Two Methods for Constructing Irreducible Polynomials over Finite Fields based on Polynomial Composition," *Proceedings of 7th International Conference on Computer Science and Information Technologies (CSIT'2009),* pp. 163-166, 2009.

[5] M. G. Evoyan, G. M. Kyureghyan and M. K. Kyuregyan, "On k-switching of mappings on Finite Fields," *Transactions of IIAP of NAS of RA, Mathematical Problems of Computer Science,* vol. 37, pp. 5-12, 2013.

[6] M. G. Evoyan, "On a Class of Permutations of Finite Field," *The Reports of National Academy of Sciences of Armenia,* vol. 113, no. 1, pp. 48-52, 2013.

РЕЗЮМЕ

Микаел Гагикович Эвоян

Методы построения неприводимых и перестановочных многочленов над конечными полями

Данная диссертационная работа посвящена исследованию неприводимых и перестановочных многочленов над конечными полями. Известно, что эти многочлены широко используются в криптографии, теории кодирования, компьютерной алгебре. С развитием современных компьютерных технологий возникает необходимость построения более мощных (многоэлементных) конечных полей, а это возможно только с помощью неприводимых многочленов. В настоящее время существуют два принципиально разных подхода к решению задачи построения неприводимых многочленов над конечными полями.

В случае первого подхода произвольно выбирается один многочлен степени n из множества всех многочленовнад конечными полями. Затем, с помощью специально разработанного алгоритма проводится проверка неприводимости многочлена. Поиск продолжается до тех пор, пока будет найден неприводимый многочлен. Недостатком этого метода являются большие требования к вычислительным мощностям для поиска неприводимых многочленов высокой степени. Второй подход – это суперпозиция или композиционный метод, основанный на свойствах конечного поля. Задача построения неприводимых многочленов с помощью композиционного метода является одной из сложных задач в теории конечных полей.

В последние десятилетия перестановочные многочлены получили широкое применение в области криптографии и теории кодирования. Несмотря на то, что исследования перестановочных многочленов ведутся с XIX в., их построение считается одной из самых сложных задач в теории конечных полей.

Целью данного исследования является изучение метода построения неприводимых и перестановочных многочленов над конечными полями и предложение новых методов построения новых классов неприводимых и перестановочных многочленов над конечными полями. Ниже представлено краткое описание полученных результатов.

1. Разработаны новые методы подробного построения неприводимых многочленов над конечными полями. Предложены методы построения неприводимых многочленов степени pt вида

$$f_t(x) = \sum_{u=0}^{p-1} \alpha^u x^{(p-u)t} - \alpha,$$

степени $p(p-1)$вида

$$\sum_{u=0}^{p-1} (ax-\beta)^u x^{(p-1-u)p} - \alpha$$

и степени ntp вида $P(x^{pt} - x^t)$. Предложен метод построения неприводимых многочленов степени n из неприводимого многочлена $P(x) = \sum_{u=0}^{n} a_u x^u$, в котором используется многочлен вида

$$g_P(x) = \sum_{\substack{0 \le j \le n \\ u+v=2j, v<u \le n}} ((-1)^u 2a_u a_v + (-1)^j a_j^2) x^j.$$

Также предложен метод построения примитивных многочленов вида

$$\sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^{u+1} a_u a_{2j-u} x^j \delta^{n-j}$$

из примитивного многочлена $P(x) = \sum_{u=0}^{n} a_u x^u$,[1, 2, 3].

2. Разработаны новые методы подробного построения неприводимых многочленов, где используются $(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta)) \times \left(h^*(x-\gamma)\right)^{-1}$и $F(x) = x^n \Psi\left(\frac{x^{q^{n+1}}+x^{q^n}+1}{x}\right)$, композиционные методы для построения новых классов неприводимых многочленов степени $n(q^n-1)$ и $n(q^n+1)$ надполем F_q, где q степень простого числа, [4].
3. Описаны и исследованы k-обмены отображений конечных полей и их свойства. Представлен метод построения перестановки многочленов типа $F(\mathrm{x}) = \gamma_1 f_1(x) + \gamma_2 f_2(x) + \cdots + \gamma_n f_n(x)$, который позволяет построить новые классы перестановочных многочленов и также их инверсионное отображение. Также исследованы многочлены вида $f_{a,b,\alpha,k}(x) = ax^q + bx + \alpha(x^q + x)^k$ над полями F_{q^2}. Даны два критерия их перестановочности, [5][6].

Полученные результаты имеют теоретическое 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 CSIT (Армения, Ереван).

ABSTRACT

Mikayel Evoyan

Construction methods of irreducible and permutation polynomials over finite fields

The purpose of present thesis is study of irreducible and permutation polynomials via composition methods over finite fields. The irreducible and permutation polynomials are known to be widely used in cryptography, coding theory and computer algebra. However, development of up-to-date computer technologies supports a necessity to construct stronger (poly-elemental) finite fields, and that can be achieved only with irreducible polynomials. Currently, there are two fundamentally different approaches to solving the problem of constructing irreducible polynomials over finite fields.

In the case of the first approach, one polynomial of degree n in is randomly selected from the set of all polynomials over finite fields. Then, through a specially developed algorithm; the polynomial is checked for being irreducible. The process is repeated until an irreducible polynomial is found. The disadvantage of this method is the high requirements towards the processing power when finding irreducible polynomials of higher degrees. The second approach is superposition or composition method, which is based on properties of the finite field. The composition methods,in terms of computation, have lower complexity. The problem of construction of irreducible polynomials via the composition method is one of the most complex problems of the theory of finite fields.

In recent decades, permutation polynomials gained a wide recognition in cryptography and coding theory. Despite the fact that permutation polynomials have been studied since XIX century, 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 and permutation polynomials over finite fields and suggesting new methods of construction of new classes of irreducible and permutation polynomials over finite fields.

A brief description of the results obtained is given below.

1. New methods of explicit construction of irreducible polynomials over finite fields are proposed. Methods for constructing irreducible polynomials of form

$$f_t(x) = \sum_{u=0}^{p-1} \alpha^u x^{(p-u)t} - \alpha$$

and degree pt, form

$$\sum_{u=0}^{p-1}(ax-\beta)^u x^{(p-1-u)p}-\alpha$$

and degree $p(p-1)$ and of degree ntp and from $P(x^{pt}-x^t)$ are given. A method for using

$$g_P(x)=\sum_{\substack{0\le j\le n\\ u+v=2j,v<u\le n}}((-1)^u 2a_u a_v+(-1)^j a_j^2)x^j$$

polynomial for the construction of irreducible polynomials of degree n from irreducible polynomial $P(x)=\sum_{u=0}^{n}a_u x^u$ is introduced. Also a method of constructing primitive polynomial

$$\sum_{j=0}^{n}\sum_{u=0}^{2j}(-1)^{u+1}a_u a_{2j-u}x^j\delta^{n-j}$$

of degree n from a primitive polynomial $P(x)=\sum_{u=0}^{n}a_u x^u$ is proposed,[1, 2, 3]..

2. Novel methods of explicit construction of irreducible polynomials are proposed, where $(x-\gamma)^n f((x-\gamma)^{-1}(x^{q^n}+\beta))\times\left(h^*(x-\gamma)\right)^{-1}$ and $F(x)=x^n\Psi\left(\frac{x^{q^n+1}+x^{q^n}+1}{x}\right)$ composition methods are used to construct new classes of irreducible polynomials of degrees $n(q^n-1)$ and $n(q^n+1)$ over F_q , where q is a power of a prime, [4].
3. k-switchings of mappings on finite fields are described and studied. A method of constructing permutation polynomials of $F(\mathrm{x})=\gamma_1 f_1(x)+\gamma_2 f_2(x)+\cdots+\gamma_n f_n(x)$ type is introduced. This allows to construct new classes of permutation polynomials and their inverce mappings. Polynomials of $f_{a,b,\alpha,k}(x)=ax^q+bx+\alpha(x^q+x)^k$type over F_{q^2} are studied. Two criteria of them being permutation polynomials on F_{q^2} are given,[5][6].

The obtained results have theoretical and practical value and can be used in both cryptography and coding theories. Six publications were made in the frame of this research and then presented at a number of conferences including CSIT (Armenia, Yerevan).