ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Մինասյան Աշոտ Վալերիի

Գծայնացվող ծածկույթներ վերջավոր դաշտերում

ՍԵՂՄԱԳԻՐ

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

ԵՐԵՎԱՆ – 2018

ЕРЕВАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Минасян Ашот Валерьевич

Линеризованные покрытия над конечными полями

АВТОРЕФЕРАТ

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

ЕРЕВАН – 2018

Ատենախոսության թեման հաստատվել է Երևանի պետական համալսարանում:

Գիտական ղեկավար՝ ֆիզ.-մաթ. գիտ. դոկտոր Ա. Ա. Ալեքսանյան
Պաշտոնական ընդդիմախոսներ՝ ֆիզ.-մաթ. գիտ. դոկտոր Լ. Հ. Ասլանյան
ֆիզ.-մաթ. գիտ. թեկնածու Վ.Պ. Գաբրիելյան

Առաջատար կազմակերպություն՝ Ինֆորմատիկայի եվ ավտոմատացման պրոբլեմների ինստիտուտ

Պաշտպանությունը կայանալու է 2018թ. հունիսի 12-ին, ժ. 16:00-ին ԵՊՀ-ում գործող ԲՈՀ-ի 044 «Մաթեմատիկական կիբեռնետիկա» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ 0025, Երևան, Ալ. Մանուկյան 1:

Ատենախոսությանը կարելի է ծանոթանալ ԵՊՀ-ի գրադարանում:

Սեղմագիրն առաքված է 2018թ. մայիսի 11-ին:
Մասնագիտական խորհրդի
գիտական քարտուղար,
ֆիզ.-մաթ.գիտ. դոկտոր՝ Վ.Ժ. Դումանյան

Тема диссертации утверждена в Ереванском государственном университете.

Научный руководитель: доктор физ.-мат. наук А. А. Алексанян
Официальные оппоненты: доктор физ.-мат. наук Л. А. Асланян
кандидат физ.-мат. наук В. П. Габриелян
Ведущая организация: Институт проблем информатики и автоматизации

Защита состоится 12-го июня 2018г. в 16:00 часов на заседании действующего в Ереванском государственном университете специализированного совета ВАК 044 “Математическая кибернетика”, по адресу: Ереван 0025, ул. А. Манукяна, 1.

С диссертацией можно ознакомиться в библиотеке Ереванского государственного университета.

Автореферат разослан 11-го мая 2018г.

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

Աշխատանքի ընդհանուր նկարագիրը

Թեմայի արդիականություն: Բուլյան ֆունկցիաների դիզյունկտիվ նորմալ ձևերը դիսկրետ մաթեմատիկայի և մաթեմատիկական կիբեռնետիկայի հիմնական, հետազոտման առարկաներից են: Դրանք լայն կիրառություն ունեն գիտության և տեխնիկայի բազմաթիվ ոլորտներում: Դիզյունկտիվ նորմալ ձևերի տեսությունը լուրջ զարգացում ապրեց անցած դարի կեսերին Ս. Յաբլոնսկու, Յու. Ժուրավլյովի, Ա. Սապոժենկոյի, Յու. Լ. Վասիլևի, Օ. Լուպանովի, Լ. Ասլանյանի աշխատանքներում: Հետագայում Ա. Անդրեևը և Ա. Կորշունովը շարունակեցին զարգացնել այդ տեսությունը՝ ստանալով կարճագույն դիզյունկտիվ նորմալ ձևերի ասիմպտոտիկ արժեքը համարյա բոլոր բուլյան ֆունկցիաների համար:

Առաջացան դժվարություններ այդ արդյունքները կիրառական խնդիրներ լուծելու ժամանակ: Այդ դժվարությունները կապված էին ոչ թե սկզբնական խնդրի, այլ դիզյունկտիվ նորմալ ձևերի մոդելի հետ, որը թույլ չէր տալիս կիրառել հանրահաշվական մոտեցումներ:

Տրամաբանական ֆունկցիաների հնարավոր պարզ դիզյունկտիվ նորմալ ձևերով իրականացման վրա են հիմնված ինտեգրալ սխեմաների նախագծման և անսարքությունների հայտնաբերման հիմնական կիրառական մեթոդները: Կան բավական մեծ թվով դիսկրետ էքստրեմալ խնդիրներ, որոնք հանգեցվում են ոչ գծային բուլյան հավասարումների լուծման: Այդ խնդիրների լուծմանն էր ուղղված դիզյունկտիվ նորմալ ձևերով տրամաբանական ֆունկցիաների ներկայացման հիմնական կիրառությունը: Այսպիսով անհրաժեշտ էր նոր մոտեցում, նոր մաթեմատիկական մոդել, որը հնարավորություն կտար տեղաշարժ գրանցել դիզյունկտիվ նորմալ ձևերի տեսության մեջ:

Յու. Ժուրավլյովը առաջարկել էր որպես այդպիսի մոդել դիտարկել գծային ֆունկցիաների արտադրյալները՝ որպես n-չափանի միավոր խորանարդի գագաթների բազմութունների՝ ինտերվալների ընդհանրացում: Դա իրականացվեց նրա աշակերտ Ա. Ալեքսանյանի կողմից[1,2,3]: Կառուցվեց գծայնացվող դիզյունկտիվ

[1] Алексанян А., Дизъюнктивные нормальные формы над линейными функциями (Теория и приложения), Ереванский государственный университет 1990.
[2] Алексанян А., Реализация булевых функций дизъюнкциями произведений линейных форм, Докл.АН СССР , т. 304, 4, 1989, стр.781-784.
[3] Алексанян А., О реализации квадратичных булевых функций системами линейных уравнений, “Кибернетика”, 1, 1989, стр.9-14.

նորմալ ձևերի տեսությունը՝ սովորական դիզյունկտիվ նորմալ ձևեի տեսության բնական ընդհանրացումը և հիմնավորվեց, որ այն ադեկվատ տեսություն է:

Տրամաբանական ֆուկցիաները նոր տեսության մեջ ներկայացվում էին ոչ թե n-չափանի միավոր խորանարդի գագաթների բազմությունների՝ ինտերվալների ծածկույթով, այլ F_{2^n} վերջավոր դաշտի գծային ենթատարածությունների հարակից դասերի ծածկույթով՝ գծայնացվող ծածկույթով: Սա հնարավորություն տվեց գրանցել բուլյան ֆունկցիաների մինիմիզացիայի էական առաջընթաց, որը անհնար էր հին տեսության մեթոդներով: Այսպիսի օրինակ է քառակուսային բազմանդամներով ներկայացվող բուլյան ֆունկցիաների դասը: Այդ դասի ֆունկցիաների կարճագույն գծայնացվող ծածկույթները հաջողվեց դուրս գրել բացահայտ բանաձևային տեսքով: Ա. Ալեքսանյանի աշխատանքները հիմնադրեցին բուլյան ֆունկցիաների հետազոտման նոր ուղղություն:

Պարզվեց որ գծայնացվող ծածկույթների գաղափարը հնարավոր է կիրառել վերջավոր դաշտում տրված բազմանդամների, ինչպես նաև վերջավոր դաշտերի ենթաբազմությունների համար: Բուլյան ֆունցիաների համար ստացված հիմնական արդյունքները հաջողվեց տարածել վերջավոր դաշտերում սահմանված ֆունկցիաների համար Ա. Ալեքսանյանի, Վ.Գաբրիելյանի և այլոց աշխատանքներում [4,5,6,7,8]:

Բուլյան ֆունկցիաների ներկայացումը դիզյունկտիվ նորմալ ձևերով էապես տարբերվում էր տրամաբանական տարրերով սխեմաների ներկայացումից, քանի որ

---

[4] Алексанян А., Серобян Р., Покрытия, связянные с квадратичными над конечным полем уравнениями, Докл.АН Арм.ССР , т. 93, 1, 1992, стр.6-10.

[5]Aleksanyan and M. Papikian, On Coset Coverings of Solutions of Homogeneous Cubic Equations over Finite Fields, The Electronic Journal of Combinatorics, 8 (2001), R22, pp. 1-9.

[6] Alexanian A., Gabrielyan V., Coverings of Symmetric Subsets in Finite Fields with Cosets of Linear Subspaces, Algebra, Geometry & Their Applications, Seminar Proceedings, vol. 3-4, 2004, Yerevan State University, pp. 110-124.

[7] Габриелян В., О метрических характеристиках, связанных с покрытиями подмножеств конечных полей смежными классами линейных подпространств, Институт проблем информатики и автоматизации, Препринт НАН РА 04-0602, Ереван, 2004.

[8] Габриелян В., О сложности покрытия системой смежных классов одного уравнения над конечным полемметрических характеристиках, связанных с покрытиями подмножеств конечных полей смежными классами линейных подпространств”, Институт проблем информатики и автоматизации, Препринт НАН РА 04-0603, Ереван, 2004.

ամենաբարդ ֆունկցիայի դիզյունկտիվ նորմալ ձևի երկարությունը էապես մեծ է «համարյա բոլոր» ֆունկցիաների բարդությունից, մինչդեռ սխեմաների դեպքում ամենաբարդ և համարյա բոլոր ֆունկցիաների բարդությունները միևնույն կարգի են: Գծայնացվող դիզյունկտիվ նորմալ ձևերի դեպքում ամենաբարդ ֆունկցիայի կառուցումը հեշտ չէ՝ սա բաց խնդիր է: Անհայտ է մնում նաև արդյոք ամենաբարդ ֆունկցիայի բարդությունը գծայնացվող դիզյունկտիվ նորմալ ձևերի դասում տարբերվում է «համարյա բոլոր» ֆունկցիաների բարդությունից:

Այսպիսով արդի խնդիր է բազմությունների նոր դասերի կարճագույն գծայնացվող ծածկույթների հետազոտումը:

Աշխատանքի նպատակը: Ատենախոսության հիմնական նպատակն է.

- Վերջավոր դաշտերի ենթաբազմությունների նոր դասերի նկարագրում, որոնց համար լուծելի է կարճագույն գծայնացվող ծածկույթի կառուցման խնդիրը:
- Դիտարկել վերջավոր դաշտից տարրերով մատրիցների գծայնացվող ծածկույթներ:
- Հետազոտել ընդհանուր աֆինական խմբի գործողությունը վերջավոր դաշտի ենթաբազմությունների վրա և դրա կապը գծայնացվող ծածկույթների բարդության հետ:

Հետազոտման օբյեկտը: Աշխատանքի հետազոտման օբյեկտը վերջավոր դաշտերի ենթաբազմությունների գծայնացվող ծածկույթներն են:

Հետազոտման մեթոդները: Աշխատանքում օգտագործված են դիսկրետ մաթեմատիկայի և հանրահաշվի մեթոդները:

Արդյունքի գիտական նորությունը: Աշխատանքի հիմնական արդյունքներն են՝

- $\dot{F}_q^n$-ով նշանակենք F_q^n գծային տարածության ոչզրոյական վեկտորների բազմությունը: Ստացվել են $\dot{F}_q^n \times \dot{F}_q^m$ դեկարտյան արտադրյալի կարճագույն գծայնացվող ծածկույթի վերին և ստորին գնահատականներ: Մասնավորապես, եթե և n-ը և m-ը 2-ի աստիճան են, ապա կարճագույն գծայնացվող ծածկույթի երկարությունը չի գերազանցում $m^{\log_2 3}\frac{n}{m}(q-1)^2$-ը: Որպես ստորին գնահատական ցույց է տրվել, որ $\dot{F}_q^n \times \dot{F}_q^m$-ի գծայնացվող ծածկույթը պարունակում է առնվազն $n(q-1)(q-\frac{1}{q^{m-1}})$ հարակից դաս:

- Ուսումնասիրվել է F_2 դաշտի վրա տրված $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ հավասարման լուծումների բազմության գծայնացվող ծածկույթները: Տրիվյալ գծայնացվող ծածկույթի երկարության կարգը n^2 է: Օգտագործելով հարակից դասերով ծածկույթների և արգելափակող բազմությունների միջև կապը՝ հաջողվել է ստանալ կարգով փոքր գծայնացվող ծածկույթ, որի երկարությունը չի գերազանցում $9n^{log_2 3} + 4$:

- Ուսումնասիրվել է F_q դաշտի վրա տրված $n \times n$ չափի վերասերված մատրիցների բազմության գծայնացվող ծածկույթները: Օգտագործելով վերասերված մատրիցների բազմության մեջ ընկած մաքսիմալ հարակից դասերի նկարագրությունը՝ հաջողվել է ստանալ կարճագույն գծայնացվող ծածկույթ, որը պարունակում է $\frac{q^n-1}{q-1}$ հարակից դաս:

- Ուսումնասիրվել է F_q դաշտի վրա տրված $n \times n$ չափի չվերասերված մատրիցների բազմության գծայնացվող ծածկույթները: Հաջողվել է ստանալ կարճագույն գծայնացվող ծածկույթ, որի երկարությունը հավասար է $(q^n-1)(q^{n-1}-1)\cdots(q-1)$:

- $xA + b$ տեսքի արտապատկերումների բազմությունը, որտեղ A-ն $n \times n$ չափի մատրից է տրված F_q դաշտի վրա, իսկ b-ն վեկտոր է F_q^n-ից, կոչվում է Աֆինական ձևափոխությունների խումբ: Ուսումնասիրվել է այդ խմբի գործողությունը F_q^n-ի ենթատարածությունների վրա: Ստացվել է, որ համարժեքության դասերի քանակը կարգով հավասար է $\frac{2^{q^n}}{A_n}$, որտեղ $A_n \approx q^{n^2+n}$ խմբի տարրերի քանակն է: Որպես հետևանք ստացվել է, որ համարյա բոլոր համարժեքության դասերը ունեն մաքսիմալ A_n չափ:
- Ստացվել է վերին գնահատական F_q^n-ի ենթատարածությունների գծայնացվող ծածկույթների համար, որը արտահայտվում է Աֆինական ձևափոխությունների խմբի տերմիններով: Ցանկացած $N \subseteq F_q^n$ բազմության կարճագույն գծայնացվող ծածկույթի երկարությունը չի գերազանցում $CR(G) \times \#orb_G(N)$ թիվը՝ $Stab(N)$-ի ցանկացած G ենթախմբի համար, որտեղ $CR(G)$-ն G-ի կարճագույն գծայնացվող ծածկույթի երկարությունն է, $Stab(N)$-ը N-ի ստաբիլ խումբը, իսկ $\#orb_G(N)$-ն ուղեծրերի քանակը:

Ատենախոսության բոլոր արդյունքները նոր են և ստացվել են հեղինակի կողմից առաջին անգամ:

Կիրառական նշանակությունը: Աշխատանքի արդյունքները ու մեթոդները կարելի է կիրառելի վերջավոր դաշտերում ոչ գծային հավասարումների համակարգերի լուծման, վերջավոր դաշտերում բազմանդամներով նկարագրված ֆունկցիաների, վերջավոր դաշտերի ենթաբազմությունների «հարմար» ներկայացում կառուցելու, ինտեգրալային սխեմաների նախագծման և թեստավորման համար, ինչպես նաև դիսկրետ մաթեմատիկայի և մաթեմատիկական կիբեռնետիկայի այլ խնդիրների հետազոտման ժամանակ:

Ապրոբացիան: Աշխատանքի հիմնական արդյունքները հրատարակված են 6 հոդվածներում: Դրանք զեկուցվել են ԵՊՀ Ինֆորմատիկա և կիրառական մաթեմատիկայի ֆակուլտետի Դիսկրետ մաթեմատիկայի և տեսական ինֆորմատիկայի ամբիոնի սեմինարում:

Աշխատանքի ծավալը և կառուցվածքը: Աշխատանքի ծավալը կազմում է 73 էջ: Աշխատանքը բաղկացած է ներածությունից, հինգ գլուխներից, եզրակացությունից և գրականության ցանկից (19 անուն):

Աշխատանքի բովանդակությունը

Գլուխ 1-ինում նկարագրված է խնդրի ընդհանուր դրվածքը և հիմնական արդյունքները, որոնք ստացվել են Ա.Ալեքսանյանի, Վ. Գաբրիելյանի կողմից: Իսկզբանե գծայնացվող ծածկույթները դիրտարկվել են, որպես բուլյան ֆունկցիաների համակարգերի էֆֆեկտիվ լուծման մեթոդ, հետագայում տեսությունը ընդհանրացվել է վերջավոր դաշտերի ենթաբազմությունների և վերջավոր դաշտերի վրա որոշված բազմանդամների վրա:

F_q-ով նշանակենք q էլեմենտ պարունակող վերջավոր դաշտը, իսկ F_q^n-ով F_q-ի վրա տրված n չափի գծային տարածությունը:

Դիցուք L-ը F_q^n-ի գծային ենթատարածություն է և $\alpha \in F_q^n$: $\alpha + L = \{\alpha + x \mid x \in L\}$ բազմությունը կոչվում է L գծային ենթատարածության **հարակից դաս**, որի չափը սահմանվում է որպես L գծային ենթատարածության չափ (նշանակվում է $dim(L)$):

Դիցուք $N \subseteq F_q^n$: Եթե $H_1, H_2, \cdots, H_s$-ը հարակից դասեր են, որոնք ընկած են N-ի մեջ, ընդ որում՝ $H_1 \cup H_2 \cup \cdots \cup H_s = N$, ապա կասենք որ $\{H_1, H_2, \cdots, H_s\}$-ը հանդիսանում է N-ի գծայնացվող ծածկույթ**:** Ծածկույթին պատկանող հարակից դասերի քանակը՝ այսինքն s-ը, կոչվում է ծածկույթի երկարություն կամ բարդություն:

Դիցուք $L \subseteq N$ հարակից դաս է: Կասենք, որ այն **մաքսիմալ հարակից դաս** է N-ում, եթե կամայական $H \subseteq N$ հարակից դասի համար $L \subseteq H$-ից հետևում է որ $L = H$. Այսինքն մաքսիմալ հարակից դասը ընկած չէ ավելի մեծ հարակից դասի մեջ:

F_q^n-ի $n-1$ չափի հարակից դասերը կանվանենք **հիպերհարթություն:**

$\dot{F}_q^n$-ով նշանակենք F_q^n-ի ոչ զրոյական վեկտորների բազմությունը:

$$\dot{F}_q^n = F_q^n \backslash \{(0, \cdots, 0)\}$$

$S \subseteq F_q^n$ բազմությունը կանվանենք ***k*-արգելափակող բազմություն**, եթե այն ունի հատում F_q^n-ի կամայական k չափի հարակից դասի հետ:

Գլուխ 2-րդի 2-րդ մասում նկարագրվում է կապը $(n-1)$-արգելափակող բազմությունների և հարակից դասերով ծածկույթների մեջ: Հայտնի է, որ $\dot{F}_q^n$-ում կարճագույն գծայնացվող ծածկույթ գտնելու խնդիրը համարժեք է F_q^n-ում մինիմալ $(n-1)$-արգելափակող բազմություն գտնելու խնդրին[9]: Այդ փաստը օգտագործվել է $\dot{F}_q^n$-ի համար $n(q-1)$ չափի հարակից դասերով կարճագույն ծածկույթ ստանալու համար:

Գլուխ 2-րդի 3-րդ մասում նկարագրվում են արդյունքներ $\dot{F}_q^n \times \dot{F}_q^m$ դեկարտյան արտադրյալ բազմության գծայնացվող ծածկույթների վերաբերյալ: Հետևյալ պնդումով նկարագրվում են այդ բազմության մեջ ընկած մաքսիմալ հարակից դասերը:

Պնդում 2.3.3: Եթե A-ն մաքսիմալ հարակից դաս է $\dot{F}_q^n \times \dot{F}_q^m$-ում, ապա $A = A_1 \times A_2$, որտեղ A_1-ը հարակից դաս է $\dot{F}_q^n$-ում, A_2-ը հարակից դաս է $\dot{F}_q^m$-ում, $dim(A_1) = n-1, dim(A_2) = m-1$:

$C_{n,m,q}$-ով նշանակենք $\dot{F}_q^n \times \dot{F}_q^m$ կարճագույն գծայնացվող ծածկույթի երկարությունը: Ակնհայտ է, որ $C_{n,m,q} \leq nm(q-1)^2$:

Պնդում 2.3.4: $C_{n,1,q} = n(q-1)^2$:

[9] Jamison R. Covering finite fields with cosets of subspaces, J. Combin. Theory Ser. A22 (1977), 253-266.

Պարզվում է, որ եթե $n > 1$ կամ $m > 1$, ապա $\dot{F}_q^n \times \dot{F}_q^m$-ի կարճագույն գծայնացվող ծածկույթի երկարության ավելի լավ գնահատականներ կարելի է ստանալ:

Պնդում 2.3.5: $C_{2n,2m,q} \leq 3C_{n,m,q}$:

Օգտագործելով Պնդում 2.3.5 ստանում ենք վերևից գնահատական $C_{n,m,q}$-ի համար:

Թեորեմ 2.3.6: Եթե $n \geq m$ և երկուսն էլ 2-ի աստիճան են, ապա $C_{n,m,q} \leq m^{log_2 3} \frac{n}{m}(q-1)^2$:

Հաջորդ թեորեմը տալիս է ստորին գնահատական $C_{n,m,q}$-ի համար:

Թեորեմ 2.3.7: $C_{n,m,q} \geq n(q-1)(q - \frac{1}{q^{m-1}})$:

Հաջորդ արդյունքները ճշգրտում են գնահատականները որոշ մասնավոր դեպքերում:

Թեորեմ 2.3.8: $C_{n,2,q} \leq 3\left\lceil \frac{n}{2} \right\rceil (q-1)^2$:

Նախորդ թորեմներից հետևում է, որ $11 \leq C_{2,2,3} \leq 12$:

Թեորեմ 2.3.9: $C_{2,2,3} = 12$:

Գլուխ 2-րդի 4-րդ մասում կառուցվում է գծայնացվող ծածկույթ F_2 դաշտի վրա տրված $x_1x_2 \cdots x_n + x_{n+1}x_{n+2} \cdots x_{2n} + x_{2n+1}x_{2n+2} \cdots x_{3n} = 1$ հավասարման համար: Տրիվյալ ծածկույթը պարունակում է $3n^2$ հատ $2n-2$ չափի հարակից դասեր: Օգտագործելով կապը $(n-2)$-արգելափակող բազմությունների և հարակից դասերով հատուկ տիպի ծածկույթների մեջ՝ հաջողվել է գտնել հավասարման լուծումների բազմության կարգով ավելի լավ գնահատական:

Թեորեմ 2.4.1: $\dot{F}_2^n$-ում մինիմալ $(n-2)$-արգելափակող բազմության հզորությունը չի գերազանցում $3n^{log_2^3}$:

Պնդում 2.4.6: $\dot{F}_2^n$-ի հիպերհարթություններով k երկարության ծածկույթի գոյությունը, այնպես որ ցանկացած 2 ոչզորյական վեկտոր ընկած են առնվազն մի հիպերհարթության մեջ, համարժեք է $\dot{F}_2^n$-ում k երկարության $(n-2)$-արգելափակող բազմության գոյությանը:

$x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ հավասարման գծայնացվող ծածկույթ գտնելու խնդիրը բերվում է $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} = 0$ հավասարման համար գծայնացվող ծածկույթ գտնելուն: Այն համարժեք է հիպերհարթություններով հատուկ տիպի ծածկույթներ գտնելու խնդրին, որն էլ ինչպես նախորդ թեորեմն է պնդում համարժեք է $\dot{F}_2^n$-ում $(n-2)$-արգելափակող բազմություն գտնելուն: Համարժեքությունների այս շղթայի միջոցով հաջողվել է կառուցել գծայնացվող ծածկույթ $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ հավասարման համար:

Պնդում 2.4.7: F_2 դաշտի վրա տրված $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ հավասարման կարճագույն գծայնացվող ծածկույթի չափը չի գերազանցում $9n^{log_2 3} + 4$:

$n^{log_2 3} \approx n^{1.58}$, հետևաբար սա կարգով ավելի լավ գնահատական է, քան տրիվյալ n^2 գնահատականը:

Գլուխ 3-րդում դիտարկվում են գծայնացվող ծածկույթներ վերջավոր դաշտի վրա տրված մատրիցների բազմության ենթաբազմությունների համար:

F_q վերջավոր դաշտի վրա տրված $n \times n$ չափի մատրիցների բազմությունը նշանակենք $M_n(F_q)$-ով: Այն n^2 չափի գծային տարածություն է F_q դաշտի նկատմամբ:

$m \in M_n(F_q)$ մատրիցը կոչվում է **վերասերված (չվերասերված)**, եթե մատրիցի դետերմինանտը 0 է (դետերմինանտը 0 չէ): Կառուցվել են կարճագույն գծայնացվող ծածկույթներ $M_n(F_q)$-ի այդ երկու ենթաբազմությունների համար:

Վերասերված մատրիցների բազմության մաքսիմալ հարակից դասերը հետազոտված և դասակարգված են[10,11,12]:

Ապացուցված է, որ այդտեղ մաքսիմալ հարակից դասերը $n(n-1)$ չափի են: Դրանցից յուրաքանչյուրում կամ բոլոր մատրիցներն ունեն տողային կախվածություն (կանվանենք տողային հարակից դասեր), կամ բոլոր մատրիցներն ունեն սյունային

[10] Dieudonne J. Sur une generalisation du groupe orthogonal a quatre variables, Arch.Math. 1 (1949) 282-287.
[11] Clement de Seguins Pazzis. The affine preservers of non-singular matrices. Arch. Math.95 (2010), 333342
[12] Meshulam R. On the maximal rank in a subspace of matrices, 4 Jul 1984

կախվածություն (կանվանենք սյունային հարակից դասեր): Յուրաքանչյուր տողային հարակից դասի բոլոր մատրիցներ տողերը գծորեն կախված են նույն առնչությամբ:

Հաջողվել է ստանալ վերասերված մատրիցների կարճագույն գծայնացվող ծածկույթի կառուցվածքը:

Թեորեմ 3.2.4: $M_n(F_q)$-ի վերասերված մատրիցների բազմության գծայնացվող ծածկույթը պարունակում է բոլոր տողային հարակից դասերը կամ բոլոր սյունային հարակից դասերը:

Մասնավորապես ցույց է տրված, որ եթե ծածկույթը չպարունակի ինչ-որ տողային հարակից դաս և ինչ-որ սյունային հարակից դաս, ապա գոյություն ունի վերասերված մատրից, որը չի ծածկվում:

Սրանից հետևում է, որ $M_n(F_q)$-ի վերասերված մատրիցների բազմության գծայնացվող ծածկույթի երկարությունը հավասար է տողային հարակից դասերի քանակին՝ $\frac{q^n-1}{q-1} = 1 + q + q^2 + \cdots + q^{n-1}$:

Գլուխ 3-րդի երրորդ մասում ուսումնասիրվել են չվերասերված մատրիցների բազմության գծայնացվող ծածկույթները: Հայտնի է, որ չվերասերված մատրիցների բազմությունը կազմում է խումբ բազմապատկման նկատմամբ և նշանակվում է $GL_n(F_q)$-ով:

$m \in M_n(F_q)$ մատրիցի սեփական արժեքների բազմությունը կոչվում է մատրիցի **սպեկտր:** Նշանակվում է $Sp(m)$: $M_n(F_q)$-ի H գծային ենթատարածությունը կանվանենք **տրիվիալ սպեկտրով**, եթե ցանկացած $m \in H$-ը մատրիցի համար $Sp(m) \subseteq \{0\}$: Այսինքն H-ի մատրիցները 0-ից տարբեր սեփական արժեքներ չունեն:

Հայտնի է[13], որ չվերասերված մատրիցների բազմության մեջ մաքսիմալ հարակից դասերը ունեն $\binom{n}{2}$ չափ և նրանց համապատասխան ենթատարածությունները տրիվյալ սպեկտրով են: Օգտագործելով այդ փաստը՝ ստացվել է հետևյալ գնահատականը:

[13] Clement de Seguins Pazzis. Large affine spaces of non-singular matrices September 24,2013

Թեորեմ 3.3.4: $GL_n(F_q)$-ի կարճագույն գծայնացվող ծածկույթի երկարությունը հավասար է $\frac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q^{\binom{n}{2}}} = (q^n-1)(q^{n-1}-1)\cdots(q-1)$:

Ծածկույթը կառուցվել է հետևայլ ձևով: $NT_n(F_q)$-ով նշանակենք խիստ վերին եռանկյունաձև մատրիցների բազմությունը: Ցույց է տրվում, որ $I_n + NT_n(F_q)$-ը մաքսիմալ հարակից դաս է $GL_n(F_q)$-ում և նրան համապատասխան գծային ենթատածությունը՝ $NT_n(F_q)$-ն տրիվյալ սպեկտրով է: $GL_n(F_q)$-ի գծայնացվող ծածկույթ կարելի է ստանալ՝ օգտագործելով $I_n + NT_n(F_q)$ ենթախմբի՝ ըստ բազմապատկման ձախ հարակից դասերը:

Գլուխ 4-րդում դիտարկվում է աֆինական ձևափոխությունների խմբի գործողությունը վերջավոր դաշտերի ենթաբազմությունների վրա:

Դիցուք $x = (x_1, \cdots, x_n)$, $f(x)$-ը և $g(x)$-ը n փոփոխականից կախված բազմանդամներ են F_q^n-ում որոշված: $L_f \subseteq F_q^n$-ով նշանակենք $f(x_1, \cdots, x_n) = 0$ հավասարման լուծումների բազմությունը: f և g ֆունկցիաները կանվանենք համարժեք, եթե գոյություն ունի չվերասերված մատրից A և վեկտոր b, այնպես որ L_f-ը արտապատկերվում է L_g-ին հետևյալ ձևով՝ $L_f = xA + b$, որտեղ $x \in L_g$.

Այսպիսով $xA + b$ տեսքի աֆինական ձևափոխությունների խումբը գործում է F_q^n-ի ենթաբազմությունների վրա:

A_n-ով նշանակենք խմբի տարրերի, իսկ M_n-ով համարժեքության դասերի քանակը: A_n-ը կարգով հավասար է q^{n^2+n}: Հաջողվել է համարժեքության դասերի համար ստանալ հետևյալ գնահատականը՝

Թեորեմ 4.1.1: F_q^n-ում համարժեքության դասերի ասիմպտոտիկ քանակը, երբ գործում է աֆինական ձևափոխությունների խումբը, հավասար է՝

$$M_n \approx \frac{2^{q^n}}{A_n}:$$

Արդյունքից հետևում է, որ համարյա բոլոր ուղեծրերը ունեն մաքսիմալ A_n չափ:

Դիցուք G-ն աֆինական ձևափոխությունների խմբում ենթախումբ է: Դիտարկենք հարակից դասեր աֆինական ձևափոխությունների խմբում: G-ի կարճագույն գծայնացվող ծածկույթի երկարությունը նշանակենք $CR(G)$-ով (Coset Rank):

Դիցուք $N \subseteq F_q^n$ և $Stab(N)$-ը N-ի ստաբիլ խումբն է, երբ գործում է աֆինական ձևափոխությունների խումբը: $Stab(N)$-ի ցանկացած ենթախումբ բաժանում է այն չհատվող ուղեծրերի: Ուղեծրերի քանակը նշանակենք $\#orb_G(N)$:

Օգտագործելով աֆինական ձևափոխությունների խումբի գործողությունը՝ հաջողվել է ստանալ վերևից գնահատական կամայական բազմության կարճագույն գծայնացվող ծածկույթի համար:

Թեորեմ 4.2.3: Ցանկացած $N \subseteq F_q^n$ բազմության կարճագույն գծայնացվող ծածկույթի երկարությունը չի գերազանցում $CR(G) \times \#orb_G(N)$ թիվը՝ $Stab(N)$-ի ցանկացած G ենթախմբի համար: Վերին սահմանը հասանելի է և չի կարող լավացվել:

Գլուխ 5-րդում նկարագրված են հարակից դասերի երկու ներկայացումներ: Ներկայացումներից մեկի գծային հավասարումների համակարգն է, իսկ մյուսը այսպես կոչված արմատ բազմանդամն է: Այն սահմանվում է հետևայլ կերպ՝ F_q^n-ի յուրաքանչյուր L հարակից դասին համապատասխանեցվում է բազմանադամ,

$$P_L(x) = \prod_{a \in L}(x - a),$$

որը կոչվում է L հարակից դասի **արմատ բազմանդամ**: Պարզվում է, այն ունի հետևյալ տեսքը՝

$$p(z) = z^{q^k} + A_1 z^{q^{k-1}} + \cdots + A_k z + A_{k+1},$$

որտեղ z-ի աստիճանները q-ի աստիճան են, իսկ գործակիցները F_{q^n} դաշտից են: Արմատ բազմանդամը առանց ազատ անդամի համապատասխանում է հարակից դասի ենթատարածությանը: Այն կոչվում է Օրեի բազմանդամ[14]: Օգտագործելով Օրեի բազմանդամի հատկությունները՝ մասնավորապես գծային օպերատոր լինելը, հաջողվել է նկարագրել ալգորիթմներ, թե ինչպես մի ներկայացումից անցնել մյուսին:

[14] 0. ORE, On a special class of polynomials, Trans. Amer. Math. Sot. 35 (1933), 559-584

Ատենախոսության թեմայի շրջանակներում հրապարակված աշխատանքների ցանկ:

1. On Minmial Coset Covering of Solutions of a Boolean Equation – A.V. Minasyan, PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY 2015, 1, p. 26–30

2. Number of Orbits of Group Acting on the Sets of Solutions of Polynomial Equations – A.V. Minasyan, PROCEEDINGS OF CSIT 2017

3. An Upper Bound for the Complexity of Coset Covering of Subsets in a Finite Field - A. A. Alexanian, A. V. Minasyan, NATIONAL ACADEMY OF SCIENCES OF ARMENIA, REPORTS 2017, Volume 117, N4, p. 287-291.

4. On the Minimal Coset Covering for a Special Subset in Direct Product of Two Finite Fields - A.V. Minasyan, PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY 2017, 51(3), p. 228–232

5. On the Mimnimal Coset Coverings of the Set of Singular and of the Set of Nonsingular Matrices - A.V. Minasyan, PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY 2018, 52(1), p. 8–11

6. On two Representations of Cosets- A.V. Minasyan, ВЕСТНИК РАУ 2018, 1 p 27-31

Abstract

The theory of linearized coverings has been established by A. Alexanian as generalization of theory of Disjunctive normal forms (d.n.f) for boolean functions. Later that theory has been extended to subsets of finite fields, as well as to polynomials defined in finite fields.

Here we describe several classes for which the problem of finding the shortest linearized covering is solvable.

We investigated both singular and nonsingular subsets of matrices defined on a finite field. For both cases minimal linearized coverings are found.

It is investigated the action of Affine group of transformations on the subsets of finite fields and its connection to the length of linearized coverings.

Here are the results:

- Let $\dot{F}_q^n$ be the set of nonzero vectors of linear space F_q^n. We have obtained upper and lower bounds for the minimal linearized covering for direct product $\dot{F}_q^n \times \dot{F}_q^m$. In particular, if both n and m are powers of 2, then the length of minimal linearized covering is not more than $m^{log_2^3} \frac{n}{m}(q-1)^2$. As a lower bound it is obtained that every linearized covering of the set $\dot{F}_q^n \times \dot{F}_q^m$ contains at least $n(q-1)(q-\frac{1}{q^{m-1}})$ cosets:

- We investigated linearized coverings for the set of solutions of the equation $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ over finite field F_2. Trivial covering has order n^2. Using the connection between linearized coverings are so called blocking sets we got covering with less order that has $9n^{log_2^3} + 4$ cosets.

- We investigated linearized coverings for the set of $n \times n$ size singular matrices that are defined on the field F_q. Using description of maximal cosets in that set we get minimal linearized covering that contains $\frac{q^n-1}{q-1}$ cosets.

- Linearized coverings for the set of $n \times n$ size nonsingular matrices that are defined on the field F_q are investigated. It is obtained that minimal linearized covering has length $(q^n-1)(q^{n-1}-1)\cdots(q-1)$:

- Consider the set of maps of form $xA + b$ where A is nonsingular matrix of size $n \times n$ defined on the field F_q and b is a vector on F_q^n. The set is called group of Affine transformations. It is investigated the action of the group on subspaces of F_q^n and obtained that the order of number of equivalence classes is equal to $\frac{2^{q^n}}{A_n}$ where $A_n \approx q^{n^2+n}$ is the number of elements of the group. As a consequence, we get that almost all equivalence classes have maximal size A_n.
- It is established an upper bound of linearized coverings of subsets of F_q^n using the action of the group of Affine transformations. For every subset $N \subseteq F_q^n$ the length of minimal linearized covering does not exceed $CR(G) \times \#orb_G(N)$ for every subgroup G of $Stab(N)$ where $CR(G)$ is length of the minimal linearized covering for G, $Stab(N)$ is the stable group of G and $\#orb_G(N)$ is the number of orbits.

Резюме

Теория линеаризованных покрытий была предложена А. Алексаняном как обобщение теории дизъюнктивных нормальных форм (д.н.ф) для булевых функций. Позже эта теория была распространена на подмножества конечных полей, а также на многочлены, определенные в конечных полях.

В данной работе описаны несколько классов подмножеств конечных полей, для которых задача нахождения кратчайшего линеаризованного покрытия разрешима.

Мы исследовали множества как вырожденных, так и невырожденных матриц, определенных на конечном поле. Для обоих случаев найдены кратчайшие линеаризованные покрытия.

Исследовано действие общей аффинной группы преобразований на подмножествах конечных полей и ее связь с длиной линеаризованных покрытий.

- Пусть $\dot{F}_q^n$ - множество ненулевых векторов линейного пространства F_q^n. Мы получили верхнюю и нижнюю оценки кратчайшег линеаризованного покрытия для прямого произведения $\dot{F}_q^n \times \dot{F}_q^m$. В частности, если оба n и m являются степенями 2, то длина кратчайшего линеаризованного покрытия не больше, чем $m^{log_2 3}\frac{n}{m}(q-1)^2$. В качестве нижней оценки получается, что каждое линеаризованное покрытие множества $\dot{F}_q^n \times \dot{F}_q^m$ содержит не менее $n(q-1)(q-\frac{1}{q^{m-1}})$ смежных классов.
- Мы исследовали линеаризованные покрытия для множества решений уравнения $x_1x_2\cdots x_n + x_{n+1}x_{n+2}\cdots x_{2n} + x_{2n+1}x_{2n+2}\cdots x_{3n} = 1$ над конечным полем F_2. Тривиальное покрытие имеет порядок n^2. Используя тот факт, что линеаризованные покрытия связаны с так называемыми блокирующими множествами, получуно покрытие с меньшим порядком длины, у которого $9n^{log_2 3} + 4$ смежных классов.
- Мы исследовали линеаризованные покрытия для множества $n \times n$-мерных вырожденных матриц, которые определены в поле F_q. Используя описание максимальных классов смежности в этом множестве, получено кратчайшее линеаризованное покрытие, содержащее $\frac{q^n-1}{q-1}$ смежных класса.
- Мы исследовали линеаризованные покрытия для множества $n \times n$-мерных невырожденных матриц, определенных в поле F_q. Получено, что

кратчайшее линеаризованное покрытие имеет длину $(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$

- Рассмотрим множество отображений вида $xA + b$, где A - невырожденная матрица размера $n \times n$, определенная в поле F_q, а b вектор из F_q^n. Это множество называется общей группой аффинных преобразований. Исследуется действие группы на подпространствах F_q^n. Получено, что порядок числа классов эквивалентности равен $\frac{2^{q^n}}{A_n}$, где $A_n \approx q^{n^2+n}$ количество элементов группы. Как следствие, мы получаем, что почти все классы эквивалентности имеют максимальный размер A_n.
- Установлена верхняя граница линеаризованных покрытий подмножеств F_q^n, использующая действие группы аффинных преобразований. Для каждого подмножества $N \subseteq F_q^n$ длина минимального линеаризованного покрытия не превосходит $CR(G) \times \#orb_G(N)$ для любой подгруппы G группы $Stab(N)$, где $CR(G)$ - длина кратчайшего линеаризованного покрытие для G, $Stab(N)$- стабильная группа G и $\#orb_G(N)$ - число орбит.