ISSN 2616-7182
eISSN 2663-1326

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің

ХАБАРШЫСЫ

BULLETIN

of L.N. Gumilyov Eurasian
National University

ВЕСТНИК

Евразийского национального
университета имени Л.Н. Гумилева

МАТЕМАТИКА. КОМПЬЮТЕРЛІК ҒЫЛЫМДАР. МЕХАНИКА сериясы

MATHEMATICS. COMPUTER SCIENCE. MECHANICS Series

Серия **МАТЕМАТИКА. КОМПЬЮТЕРНЫЕ НАУКИ. МЕХАНИКА**

№1(138)/2022

1995 жылдан бастап шығады

Founded in 1995

Издается с 1995 года

Жылына 4 рет шығады

Published 4 times a year

Выходит 4 раза в год

Нұр-Сұлтан, 2022
Nur-Sultan, 2022
Нур-Султан, 2022

Редакцияның мекенжайы: 010008, Қазақстан, Нұр-Сұлтан қ., Сәтпаев к-сі, 2, 402 бөлме.
Тел: +7 (7172) 709-500 (ішкі 31-410). E-mail: *vest_math@enu.kz*

Жауапты редактор: А.Ж. Жұбанышева

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы.
МАТЕМАТИКА. КОМПЬЮТЕРЛІК ҒЫЛЫМДАР. МЕХАНИКА сериясы
Меншіктенуші: Л.Н. Гумилев атындағы Еуразия ұлттық университеті.
Мерзімділігі: жылына 4 рет.
Қазақстан Республикасы Ақпарат және қоғамдық даму министрлігімен тіркелген. 02.02.2021 ж.
№ KZ65VPY00031936 қайта есепке қою туралы куәлігі.
Типографияның мекенжайы: 010008, Қазақстан, Нұр-Сұлтан қ., Қажымұқан к-сі ,12/1,
тел: +7 (7172)709-500 (ішкі 31-410).

Editorial address: 2, Satpayev str., of. 402, Nur-Sultan, Kazakhstan, 010008.
Tel.: +7 (7172) 709-500 (ext. 31-410). E-mail: *vest_math@enu.kz*

Responsible Editor-in-Chief: Aksaule Zhubanysheva

Bulletin of the L.N. Gumilyov Eurasian National University.

MATHEMATICS. COMPUTER SCIENCE. MECHANICS Series
Owner: L.N. Gumilyov Eurasian National University. Periodicity: 4 times a year.
Registered by the Ministry of Information and Social Development of the Republic of Kazakhstan. Rediscount certificate № KZ65VPY00031936 dated 02.02.2021.

Address of printing house: 12/1 Kazhimukan str., Nur-Sultan, Kazakhstan 010008; tel: +7 (7172) 709-500 (ext.31-410).

Адрес редакции: 010008, Казахстан, г. Нур-Султан, ул. Сатпаева, 2, каб. 402
Тел: +7 (7172) 709-500 (вн. 31-410). E-mail: *vest_math@enu.kz*

Ответственный редактор: А.Ж. Жубанышева

Вестник Евразийского национального университета имени Л.Н. Гумилева.
Серия МАТЕМАТИКА. КОМПЬЮТЕРНЫЕ НАУКИ. МЕХАНИКА
Собственник: Евразийский национальный университет имени Л.Н. Гумилева.
Периодичность: 4 раза в год.
Зарегистрировано Министерством информации и общественного развития Республики Казахстан.
Свидетельство о постановке на переучет № KZ65VPY00031936 от 02.02.2021 г.
Адрес типографии: 010008, Казахстан, г. Нур-Султан, ул. Кажымукана, 12/1, тел.: +7 (7172)709-500 (вн.31-410).

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы. Математика. Компьютерлік ғылымдар. Механика сериясы, №1(138)/2022

Bulletin of L.N. Gumilyov Eurasian National University. Mathematics. Computer science. Mechanics series, №1(138)/2022

Вестник Евразийского национального университета имени Л.Н.Гумилева. Серия Математика. Компьютерные науки. Механика, №1(138)/2021

МАЗМҰНЫ
CONTENTS
СОДЕРЖАНИЕ

Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2022, Vol. 138, №1, P.6-22
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

МРНТИ: **81.93.29**

С.Е.Нысанбаева [1,2] , К.Т. Алғазы [1] , Қ.С.Сақан [1,2] , А.Хомпыш [1,2] , Д.С.Дүйсенбаев [1]

[1] *ҚР БҒМ ҒК "Ақпараттық және есептеуіш технологиялар институты" Алматы, Қазақстан*
[2] *әл-Фараби атындағы ҚазҰУ Алматы, Қазақстан*
(E-mail: 19kairat78@gmail.com)

CF блокты шифрлау алгоритмі және оны биттік шашырау эффектіне зерттеу

Аңдатпа: Мақалада қазіргі есептеу технологиялардың қарқынмен дамуы кезеңінде мәліметтердің құпиялығын қамтамасыз ету үшін қолданылатын симметриялық блокты шифрлардың маңыздылығы, ерекшеліктері және пайдалану аумағы жайлы айтылады. Осы ретте "Ақпараттық және есептеуіш технологиялар институтының" "Ақпараттық қауіпсіздік зертханасында" жасалынған CF симметриялы блокты шифрлау алгоритмінің құрылымы, оның құпия кілт негізінде раундтың кілттерді жасау механизмі айтылған. Құрылған шифрлау алгоритмінің компьютерлік бағдарламасы жасалды, соның негізінде жұмыс істеу өнімділігі зерделеніп және ашық мәтін мен шифрмәтін арасындағы "лавиндік эффект" қасиеті мен "қатаң лавиндік эффект" қасиеті тексерілді. Алгоритмді аппараттың жүзеге асырылуын оңтайландыру мақсатында сызықтық емес түйін ретінде қарастырылған S-блок ауыстыру түрлендіруі 4x4 биттік өлшемде алынды.

Кілт сөздер: шифрлау алгоритмі, алгоритмнің криптоберіктілігі, "лавиндік эффект" критерийі, "қатаң лавиндік эффект" критерийі.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.1

2000 Mathematics Subject Classification: 94-04

1. Кіріспе

Заманауи технологиялардың қарқындап дамуы кезеңінде өзекті болып саналатын бағыттардың ішіндегі ақпараттарды сақтау, сенімді жою мен алмасудағы құпиялылықты жоғарғы дәрежеде қамтамасыз ету үлкен мәселе болып отыр. Осы мақсаттағы ақпараттарды криптографиялық қорғау әдістерінің ішінде симметриялық блокты шифрлау алгоритмдерімен қорғау қазіргі уақытта заманауи ақпараттық және телекоммуникациялық жүйелерде ақпаратты өңдеу барысында құпиялылықты қамтамасыз етудің негізгі сенімді бірден-бір жолы болып табылады [1]. Сол себепті симметриялы блокты шифрлар оның жоғарғы криптоберіктілігіне және жылдамдығына байланысты шифрлаудың басқа кластарымен салыстырғанда кеңінен пайдаланады.

Бүгінгі күндері дамыған елдердің шифрлау алгоритмдері, көбінесе, симметриялық блоктық шифрлардың класына негізделген. Бәрімізге белгілі, симметриялы шифрлар класының қауіпсіздігі голланд криптографы Киркхоффстің өзі аттас принципіне негізделген, оған сәйкес кез-келген симметриялы шифрдың қауіпсіздігі шифрлау алгоритмінің құрылымының құпиялығымен емес, тек оның кілтінің құпиялығында жатыр [2-3].

Ақпараттың қауіпсіздігін қамтамасыз ету үшін криптографиялық жүйелерді қолдану технологиялық дамудың қарқынына да көп байланысты. Қазіргі таңда симметриялы блокты шифрларды қолдану, қолдану шарттары мен мүмкіндіктері саласында үнем жаңарту мен қайта қарауды талап етеді. Әдетте, бұл криптографиялық тұрақтылық,

икемділік және шифрлау жұмысының өнімділігі, сонымен бірге қазір өзекті болып тұрған аппараттық іске асырудағы баға/уақыт тиімділігі бойынша талаптарды қайта қарауға әкеледі [4].

Жасалатын шифрлау алгоритмі қауіпсіздіктің жоғары деңгейін қамтамасыз етуі, тиімді жылдамдықпен жұмыс істеуі, сондай-ақ оның бағдарламалық, аппаратты-бағдарламалық және аппараттық бағытта бізге қажетті деңгейде жүзеге асырыла алуы қажет.

Әлі күнде де блоктық шифр ақпараттың құпиялылығын қамтамасыз етудің маңызды құралы болып табылады. Көбінесе, симметриялы блокты алгоритмдердің құрылымы сызықты және сызықты емес түйіндерден тұрады. Сызықты түрлендірулер – ашық мәтін мәндерін ішінара бір-бірімен барынша жоғары деңгейде араластыру үшін, ал сызықты емес түйіндер – ақпарат пен оның шифрланған нұсқасы арасындағы байланысты барынша қиындату, яғни мейлінше жоғарғы ретті сызықты емес байланыстар орнату [5]. Тәжірибеде сызықты емес түйін мәселесін шешу ретінде S-блок ауыстырулары көп пайдаланылуда. Қазіргі уақытта радиожиілікті сәйкестендіру жүйелері (RFID) сияқты шектеулі ресурстарға ие құрылғылардың қауіпсіздігін арттыруға үлкен мәселелер туындауда. Аз ресурсты құрылғыларда көбінесе 4 биттік S-блок ауыстырулары пайдаланылады. SLIM деп аталатын RFID жүйелеріне арналған жаңа ультражеңіл криптографиялық алгоритм ұсынылған [6]. SLIM алгоритмі Фейстель желісіне негізделген 32 биттік блоктық шифр RFID жүйелері үшін қолайлы, яғни құны мен қауіпсіздігі және энергия қуатын үнемдейтін қасиетке және тамаша өнімділікке ие. Сонымен бірге, 4-биттік S-блок ауыстыруларын қолданатын PRESENT және GIFT сияқты танымал жеңілсалмақты шифрлау алгоритмдерін ауданы мен қуаты жағынан шамамен 40% аз тұтынатын S-блоктар үшін жоғары оңтайландырылған IT сұлбалары жайлы зерттеулер жүргізілген [7].

AUT64 шифрлау алгоритмі қауіпсіздікке сезімтал бірқатар қосымшаларда қолданылатын, мысалы, көлік құралдарының иммобилизациясы сияқты 120 биттік құпия кілті бар 64 биттік блоктық шифры жайлы [8] мақалада зерттеулер жүргізілген. Бұл мақалада блокты шифрлау алгоритмінің толық сипаттамасы және талдауы, онымен байланысты аутентификация хаттамасы, сондай-ақ бірқатар криптографиялық кемшіліктерді қарастырылған. Бұл жоғарғыдағы мақалалар 4-биттік S-блок ауыстыруларын шифрлау алгоритмдерінің құрылымдарында пайдалану әлі де қолданыста өзекті екендігін көрсетіп берді.

Жаңа CF шифрлау алгоритмінде оның бағдарламалы-аппараттық және аппараттық тұрғыда икемді жүзеге асырылу мақсатында және бұл алгоритмді блоктық шифрлар негізінде хеш алгоритмдерін жасауда пайдалануды ойластыра отырып, S-блок ауыстыруларын басқа жолмен іске асыру қарастырылған. Ал, S-блок заманауи блоктық шифрлау алгоритмдерінің құрылысының, соның ішінде кілт жасау алгоритмдерінің де ажырамас бөлігі болып табылады. [9] мақалада Фейстель желісіне таңдалған S-блок механизміне кеңінен тоқталған, Фейстель кілтімен таңдалған S-блок механизмінің жалпыланған нұсқасын жан-жақты қарастырған.

Қазіргі заманғы симметриялық блоктық шифрлау алгоритмдері үшін аналитикалық шабуылдарға криптографиялық төзімділікті бағалау критерийін басшылыққа ала отырып, 4-биттік бірнеше S-блокті белгіленген тәртіппен жұмыс жасататын жаңа CF симметриялық блокты шифрлау алгоримі және оның құрамдас бөлігі CFKey кілт жасау алгоритмі құрылды [10]. Енді сол алгоритмнің құрылымын және әрбір түрлендірулеріне жекелей тоқталып өтейік.

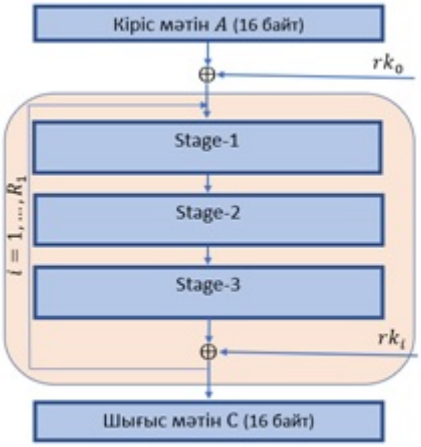
2. Негізгі нәтижелер

2.1. CF шифрлау алгоритмін әзірлеу

2.1.1. CF шифрлау алгоритмінің жалпы сұлбасы

SP желісі негізінде жасалған CF шифрлау алгоритмі ақпараттың қауіпсіздігін криптографиялық тұрғыдан қамтамасыз ету бағытында симметриялық блоктық шифрлау

алгоритмдері класына жатады. Алгоритмнің шифрлау блогінің және кілттің ұзындығы – 128 бит. Алгоритмнің құрамдас бөлігіне сызықтық түрлендірулермен қатар сызықты емес түрлендірулер де кіреді: сызықты түрлендірулер – модуль 2 бойынша биттік қосу және солға қарай циклдық жылжыту операциялары, ал сызықтық емес түрлендірулер ретінде кіріс және шығыс биттерінің көлемі 4 биттен болатын төрт S-блок алмастыруы түрлендіруі қарастырылады. Шифрдың құрылымы ауыстыру-алмастыру желісі (SP-сеть) нұсқасына жатады және шифрлау раундының саны – $R_1 = 4$. Әр шифрлау раунды Stage-1, Stage-2 және Stage-3 түрлендірулерінен тұрады. CF шифрлау алгоритмінің жалпы сұлбасы Сурет-1-де көрсетілген.



Сурет 1 – CF алгоритмі жалпы сұлбасы

Шифрлау жұмысы барысында алдымен раундтық кілтпен ағарту процесі жүргізіледі. Ең бірінші раундтық кілт ретінде негізгі құпия кілтті пайдаланамыз. Әр раундта тізбектей орындалатын Stage-1, Stage-2 және Stage-3 түрлендіруінен кейін алынған шифрмәтінді раундтық кілтпен модуль екі бойынша биттік қосу операциялары орындалып отырады. Соңғы раунд R_1 =4 аяғында 16 байтты шифрмәтін блогін аламыз. Раундтық кілттерді жасау CFKey алгоритмі арқылы іске асырылады, ол жайлы кейінірек тоқталатын боламыз. $A(a_0, a_1, a_2, \ldots, a_{15})$ кіріс мәтін 4x4 өлшемдегі квадрат матрица түрінде келесідегідей ретпен жазып алайық:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_2 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Ескере кететіні, A матрицасының бірінші жазбасында матрица элементтері индекстері кіріс мәтіннің реттік нөмірі бойынша, ал екінші жазбада матрица жолы мен бағанының индексі бойынша жазылған. Матрицаның әр элементі бір байт ретінде қарастырылады. Бұдан әрі әр түрлендірулерге жекелей тоқтала кетейік.

2.1.2. Stage-1 түрлендіруі

Аталған түрлендіру орындалу нәтижесінде берілген A матрицасының өлшеміндегідей жаңа матрица алынады. Stage-1 түрлендіруінің бір ерекшелігі болып шифрлау барысында сызықты және сызықты емес криптографиялық түйіндер қатарласып жұмыс істеуі саналады. Матицаның әр элементтерін есептеу барысында бұл екі түйіндер жұмыс кезінде төмендегідей қадамдармен анықталып, сол элемент үшін екеуі бірінен кейін бірі тізбектесіп орындалып отырады.

1-қадам. Бұл қадам сызықты түйін қадамы. A матрицасы арқылы есептелінетін c_{ij} аралық мәндері матрица құрылымы бойынша солдан оңға, жоғарыдан төмен бағытта есептелініп алынады, мұндағы, $i, j = 0, 1, 2, 3$. c_{ij} аралық мәндері есептелу тәртібі

мынандай: матрицаның i-ші жолындағы төрт элемент пен j-ші бағандағы i мен j қиылысындағы элементтен басқа үш элементтердің модуль екі бойынша биттік қосындысы аталған c_{ij} мәнін береді. Көрсетілген Сурет-2-де мысал ретінде c_{00} аралық мәнін есептеуге қатысатын матрица элементтері белгіленген.

$$c_{00} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Сурет 2 – c_{00} **- элементін есептеу жолы**

2-қадам. Бұл қадам сызықты емес түйін - S-блок ауыстыру операциясынан тұрады. 1-қадамда есептелінген c_{ij} аралық мәні S-блок ауыстырудан өтіп, A матрицасының жаңа мәні ретінде қабылданады, яғни сол орынға жазылады. S-блоктан өткізу реті SBOX процедурасы негізінде жүргізіледі. 1-қадам және 2-қадамнан тұратын Stage-1 түрлендіруін алгебралық түрде мына формуламен жазуға болады:

$$\left.\begin{array}{l} c_{ij} = \oplus \sum\limits_{k=0}^{3} a_{ik} \oplus (\oplus \sum\limits_{k=0,k\neq i}^{3} a_{kj}); \\ a_{ij} = SBOX(c_{ij}); \end{array}\right\} i,j = 0,1,2,3. \qquad (1)$$

мұндағы, c_{ij} – A матрицы арқылы есептелетін аралық мән, SBOX – S-блок ауыстыру процедурасы, $\oplus\sum$ – модуль 2 бойынша биттік қосу операциясы.

2.1.3. SBOX процедурасы

Аталған процедура S-блок ауыстыру операциясын орындайды. Бізге алдынала төрт S_0, S_1, S_2, S_3 блоктары кестемен беріледі, мұндағы $S_i : Z_{2^4} \to Z_{2^4}$, $i = 0, \ldots, 3$. Қарастыратын S_0, S_1, S_2, S_3 ретінде шифрлау алгоритмінде сызықсыздық дәрежесін максимальды етіп алу мақсатына төрт "Алтын S-блоктарды" аламыз және олар Кесте-1-де көрсетілген [11]. Шетелдік ғалымдар M.O. Saarinen және т.б. ғалымдардың еңбектерінде ондаған криптографиялық алгоритмдердің S-блоктарының дифференциалдық және сызықтық қасиеттері бойынша салыстырмалы кестесін құрды және жақсы нәтиже беретін S-блоктарды "Алтын S-блоктар" деп атады. Ұсынылып отырған алгоритмде қолданылған дайын S-блоктар осы S-блоктар топтамасынан алынды [12-14].

Кесте 1 – **Төрт "Алтын S-блоктар"**

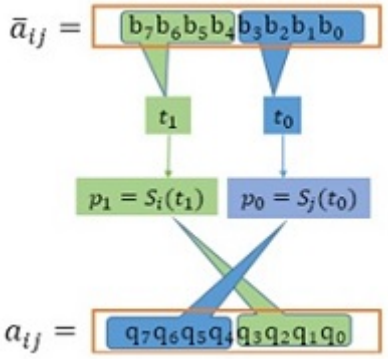
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
$S_0(x)$	0	F	B	8	C	9	6	3	D	1	2	4	A	7	5	E	Serpent, S_3
$S_1(x)$	2	E	F	5	C	1	9	A	B	4	6	8	0	7	3	D	HB-1, S_2
$S_2(x)$	7	C	E	9	2	1	5	F	B	6	D	0	4	8	A	3	HB-2, S_0
$S_3(x)$	4	A	1	6	8	F	7	C	3	0	E	D	5	9	B	2	HB-2, S_1

Ескерту: Serpent - жеңілсалмақты Serpent шифры,
HB-1 - жеңілсалмақты Hummingbird-1 шифры,
HB-2 - жеңілсалмақты Hummingbird-2 шифры.

SBOX процедурасының жұмыс істеу тәртібі төмендегідей тәртіппен анықталады: $a_{ij} = SBOX(\overline{a}_{ij})$. Өңделуге кіріс мән ретінде A матрицасының бір байты $\overline{a}_{ij}$ кіретін болсын. Бұл байттың екілік санау жүйесіндегі жазбасын былай белгілейік: $\overline{a}_{ij} = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_2$. S-блок ауыстыру операциясы жарты байттар деңгейінде жүргізіледі (ниббл (nybble) немесе тетрада). Сәйкесінше, $\overline{a}_{ij}$ байтының екілік

жазбасын оңжақты жарты байт және солжақты жарты байт деп бөліп алып, төмендегідей белгілеу енгізейік: $t_1 = b_7b_6b_5b_4$, $t_0 = b_7b_6b_5b_4$. Бұдан әрі, осы мәндер арқылы $p_1 = S_i(t_1) = (q_7q_6q_5q_4)_2$, $p_0 = S_j(t_0) = (q_3q_2q_1q_0)_2$ анықтайық. Матрицаның элементінің i мен j индекстері S-блоктың реттік нөмірлерін көрсетеді. Келесіде, i-ші және j-ші S-блоктардан алынған мәндердің екілік жазбасын конкатенация арқылы біріктіреміз. Ескере кететіні, конкатенация кезінде жарты байттар p_0 және p_1 орындарымен алмасады: алынған p_1 - солжақты жарты байт, p_0 - оңжақты жарты байт. Осындай тәртіппен алынған байт шығыс ретінде $(a_{ij})_2 = (p_0)_2 \parallel (p_1)_2$ болып анықталады. SBOX процедурасының жұмыс істеуінің графикалық нұсқасы Сурет-3-те кескінделген.

SBOX процедурасы жұмысына мысал: Бізге $\overline{a}_{32} = 32_{10} = 00100000_2 = 20_{16}$ берілсін. Онда Кесте-1 бойынша мыналарды анықтаймыз $p_1 = S_3(2_{16}) = 1_{16}$, $p_0 = S_2(0_{16}) = 7_{16}$. Бұдан әрі $a_{32} = p_0 \parallel p_1 = 71_{16} = 01110001_2 = 113_{10}$ екенін аламыз. Нәтижесінде $a_{32} = SBOX(32) = 113$ болып шығады.



Сурет 3 – SBOX процедурасы сұлбасы

2.1.4. Stage-2 түрлендіруі

Аталған Stage-2 түрлендіруі екі кезеңнің жиынтығынан тұрады: солға қарай циклдық жылжыту және модуль 2 бойынша биттік қосу (xor операциясы). Бірінші кезеңде Stage-1 түрлендіруінен алынған матрицасының 16 мәні бір өлшемді массив ретпен жазылып алынады $(a_{00}, a_{01}, a_{02}, a_{03}, a_{10}, a_{11}, a_{12}, a_{13}, a_{20}, a_{21}, a_{22}, a_{23}, a_{30}, a_{31}, a_{32}, a_{33})$. Содан әрі, бұл элементтер байт ретінде қабылданып, олардың екілік санау жүйесіндегі жазбасы конкатенация операторы арқылы біріктіріледі: $W = a_{00} \parallel a_{01} \parallel a_{02} \parallel a_{03} \parallel a_{10} \parallel a_{11} \parallel a_{12} \parallel a_{13} \parallel a_{20} \parallel a_{21} \parallel a_{22} \parallel a_{23} \parallel a_{30} \parallel a_{31} \parallel a_{32} \parallel a_{33}$, $|W| = 128$ бит. Осы тізбекке солға қарай 1 бит циклдық жылғыту орындалып, $V = W \lll 1$, алынған тізбек он алты байтты жаңа нәтиже аламыз: $V = b_{00} \parallel b_{01} \parallel b_{02} \parallel b_{03} \parallel b_{10} \parallel b_{11} \parallel b_{12} \parallel b_{13} \parallel b_{20} \parallel b_{21} \parallel b_{22} \parallel b_{23} \parallel b_{30} \parallel b_{31} \parallel b_{32} \parallel b_{33}$. Келесі кезеңде алынған V мен W массивтері xor операциясымен қосылады:

$$A = W \oplus V. \tag{2}$$

Ақырғы алынған нәтиже A матрицасының жаңа элементтері болып солдан оңға, жоғарыдан төмен ретпен жазылады.

2.1.5. Stage-3 түрлендіруі

Stage-3 түрлендіруі құрылымы жағынан жоғарыда көрсетілген Stage-1 түрлендіруіне өте ұқсас. Ол түрлендірудегідей, Stage-3 түрлендіруіндегі матрицасы мәндері бірінші – сызықты, екінші – сызықты емес криптографиялық түйінге жататын екі қадамнан тұратын операциялар арқылы есептелінеді, нәтижесінде жаңа осындай өлшемдегі матрица алынады. Жұмыс істеу тәртібіндегі өзгешелік – жаңа матрица элементтерін есептеудегі бағытта, яғни матрица элементтерін есептеу төменнен жоғарыға дейін, оңнан сол бағытта жүргізіледі. Осы жердегі S-блок ауыстырулары ретінде Кесте-1-де көрсетілген "Алтын S-блоктар" қолданылады. S-блоктар жұмыс реті SBOX процедурасымен жүзеге асырылады.

Әр элементті есептеу барысында қадам-1 мен қадам-2 тізбектеліп жүргізіледі. Есептеу матрицаның a_{33} элементінен бастап, a_{00} элементінен дейін өтеді. Қадам-1 мен қадам-2-ден тұратын есептеуді алгебралық түрде мына формулалармен жүргіземіз:

$$\left.\begin{array}{c} c_{ij} = \oplus \sum\limits_{k=0}^{3} a_{ik} \oplus (\oplus \sum\limits_{k=0,k\neq i}^{3} a_{kj}); \\ a_{ij} = SBOX(c_{ij}); \end{array}\right\} i,j = 3,2,1,0. \tag{3}$$

Аралық мән c_{ij} есептеу кезінде сәйкесінше матрицаның i-ші жолындағы төрт элемент пен j-ші бағандағы үш элементтердің (i-жол мен j-баған қиылысындағы элементтен басқа) модуль екі бойынша биттік қосындысы бойынша жүреді. Сурет-4-де мысал ретінде

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Сурет 4 – c_{33} - элементін есептеуде қатысатын элементтер

c_{33} аралық мәнін есептеуге қатысатын матрица элементтері графиктік түрде көрсетілген. Stage-3 түрлендіруі нәтижесінде аралық шифрланған 16 байтты блок аламыз.

2.1.6. CFKey раундтық кілттерді жасау алгоритмі

Бұл бөлімде 16 байт ұзындықтағы $K(k_0, k_1, k_2, \ldots k_{15})$ құпия кілттен осы ұзындықтағы раундтық кілттерді жасау алгоритмі қарастырылады. Біз K құпия кілтін K_0 раундтық кілт деп ұйғарайық. Раундтық кілттердің жалпы саны осы шифрлау алгоритміндегі R_1 раунд санына сәйкес келеді. Алдымен, $K_0(k_0, k_1, k_2, \ldots k_{15})$ раундық кілтті 4x4 өлшемдегі A квадрат матрицасы түрінде төмендегідей ретпен жазып алайық:

$$A = \begin{pmatrix} k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ k_8 & k_9 & k_{10} & k_{11} \\ k_{12} & k_{13} & k_{14} & k_{15} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

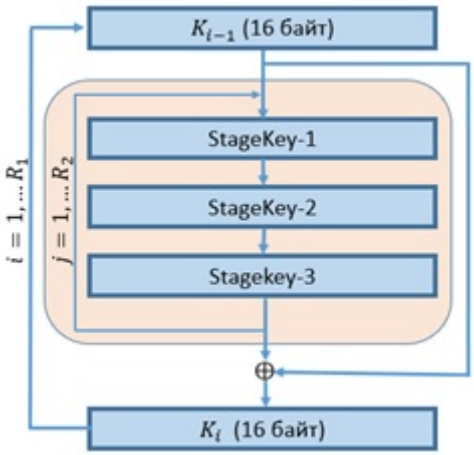
CFKey раундтық кілттерді жасау алгоритмі StageKey-1, StageKey-2 және StageKey-3 түрлендірулерінен тұрады. Ұсынылған кілт жасау алгоритмі жұмысы графикалық түрде Сурет-5-те көрсетілген. Жұмыс істеу тәртібі бойынша аталған CFKey алгоритмі CF шифрлау алгоритмімен өте ұқсас: Stage-1 түрлендіруі StageKey-1 түрендіруімен, Stage-2 түрлендіруі StageKey-2 және Stage-3 түрлендіруі – StageKey-3. Бір ғана айырмашылық – StageKey-2-де. Аталған түрлендіру Stage-2-дағыдай екі операциядан емес, тек бір ғана операциядан тұрады: солға қарай 1 бит циклдық жылжыту операциясы. CFKey алгоритмі Сурет-5-те көрсетілгендегідей келесі K_i раундтық кілтті алу үшін $R_2 = 8$ рет қайталанады, одан соң алынған нәтиже K_{i-1} раундтық кілтімен модуль 2 бойынша биттік қосылады, мұнда $i = 1, \ldots, R_1$ дейін.

2.2. CF шифрлау алгоритмінің бағдарламалық жүзеге асырылуы

Жасалған алгоритмнің бағдарламалық іске асыру жағынан жұмыстар жүргізілді, ол Delphi.7 бағдарламалық тілінде құрылып, алынған нәтижелер шифрлау алгоритмдердің негізгі сипаттамалары жағынан жан-жақты тәжірибелік тұрғыда сараланды. Құрылған бағдарлама төмендегідей функциялардың жұмыс істеуін қамтиды:

– симметриялы раундтық кілттерді жасау;
– файлдарды шифрлау;
– файлдарды кері шифрлау.

Бағдарламаның көмегімен алгоритмнің жұмыс істеу өнімділігі қарастырылды. Шифрлау процесі уақыты 1 Gb ақпаратты шифрлау үшін алдын-ала берілген 16



Сурет 5 – Раундтық кілттерді жасау алгоритмі сұлбасы

байттық ақпарат блогін 67 108 864 рет қайталап есептеу барысында алынды. Осы тәсіл нәтижесінде раунд саны $R_1 = 4$ болғанда, Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz 3.19 GHz процессорі негізінде 1 Gb ақпаратты 1 минут 23 секундта жабады. Кері шифрлау процесіне де осы көрсеткішке шамалас уақыт жұмсалды.

2.3. Әзірлеген алгоритмді қауіпсіздікке талдау

2.3.1. CF шифрлау алгоритмінің биттік шашырауын (лавиндік эффект) зерттеу

Шифрлау алгоритмін жобалау кезінде жасалатын шифр биттік шашырау әсері (лавиндік эффект) критерийін қанағатандыруы керек. Биттік шашырау әсері – шифрлау үшін маңызды криптографиялық қасиет. Бұл қасиет кіріс мәтіндегі немесе кілттегі биттердің аз мөлшердегі өзгерісі шифрмәтіннің шығыс биттерінің қажетті мөлшерде өзгеруіне әкелетінін білдіреді. Биттік шашырау әсерін зерттеу, әдетте, блоктық шифрларға қолданылады. Егер алгоритм қажетті дәрежеде биттік шашырау әсерімен қамтамасыз етілмесе, онда криптоталдаушы шығыс биттер негізінде кіріс биттер туралы ақпарат алуға мүмкіндік алады [11, 12].

Биттік шашырау әсері критерийі үшін биттік шашырау әсері параметрінің мәні мына формуламен анықталады: $\varepsilon_\alpha = |2k_i - 1|$, мұнда, i – кіріс мәндегі өзгертілген биттің нөмірі, k_i – бастапқы (өзгермейтін) кіріс мәнін шығыс мәнімен салыстырғанда кіріс мәніндегі i-ші бит өзгерген кезде шығыс мәніндегі биттердің жартысына жуығының өзгеру ықтималдығы.

CF алгоритмінің биттік шашырауын зерттеу нәтижелерін бағдарлама көмегімен алдық. Егер бір-бірінен тек 1 бит ғана өзгеше екі ашық мәтінді қарастырсақ, онда осы екі ашық мәтін шифрмәтіндері тіпті 1-ші раундтан кейінен-ақ бір-бірінен өзгеше болатынын байқаймыз. Бұл өзгерісті әрбір 1-ден 128-ге дейінгі жеке-жеке өзгерген биттер үшін төмендегі Кесте-2-ден немесе Сурет-6-дан көруге болады.

Өздеріңіз байқағандай, 1-ші раундтан кейін биттік шашырау қанағаттанарлық дәрежеде, ал енді шифрлау алгоритмінің толық 4-ші раундынан кейін де осындай көрсеткіш көрсетуі осыдан-ақ белгілі.

2.3.2. Қарастырылған S-блоктардың қатаң лавиндік эффекті қасиетіне зерттеу

Енді біз қарастырған төрт S-блоктарға қатысты қатаң лавиндік эффектіні зерттейік. Қатаң лавиндік критерийі (SAC) S-блоктарды бағалауда негізгі критерийлердің бірі болып табылады. Ол дифференциалды криптоталдауға төзімділікті сипаттайтын S-блоктарды синтездеу процесінде кеңінен қолданылады [17]. Бәрімізге мәлім, бульдік функцияларды S-блоктар құрылымының бөлігі ретінде қарастыруға болады. SAC-ті қанағаттандыратын

Кесте 2 – Биттік шашырау критерийі

i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i	i	k_i
1	0,49	17	0,49	33	0,44	49	0,55	65	0,5	81	0,47	97	0,51	113	0,46
2	0,48	18	0,5	34	0,47	50	0,51	66	0,46	82	0,5	98	0,45	114	0,53
3	0,54	19	0,45	35	0,57	51	0,5	67	0,53	83	0,46	99	0,52	115	0,43
4	0,48	20	0,5	36	0,54	52	0,54	68	0,49	84	0,53	100	0,57	116	0,55
5	0,46	21	0,53	37	0,48	53	0,53	69	0,47	85	0,47	101	0,5	117	0,39
6	0,47	22	0,42	38	0,57	54	0,49	70	0,53	86	0,5	102	0,46	118	0,54
7	0,49	23	0,42	39	0,5	55	0,46	71	0,45	87	0,48	103	0,57	119	0,53
8	0,45	24	0,46	40	0,5	56	0,55	72	0,53	88	0,53	104	0,47	120	0,50
9	0,49	25	0,53	41	0,57	57	0,5	73	0,42	89	0,45	105	0,52	121	0,48
10	0,53	26	0,46	42	0,46	58	0,51	74	0,46	90	0,46	106	0,46	122	0,50
11	0,56	27	0,46	43	0,5	59	0,47	75	0,46	91	0,52	107	0,52	123	0,52
12	0,51	28	0,48	44	0,46	60	0,42	76	0,46	92	0,46	108	0,47	124	0,46
13	0,51	29	0,50	45	0,5	61	0,55	77	0,55	93	0,53	109	0,45	125	0,5
14	0,53	30	0,5	46	0,53	62	0,54	78	0,53	94	0,46	110	0,51	126	0,45
15	0,53	31	0,47	47	0,53	63	0,45	79	0,46	95	0,53	111	0,42	127	0,44
16	0,5	32	0,45	48	0,38	64	0,55	80	0,56	96	0,55	112	0,46	128	0,5

Сурет 6 – Биттік шашырау критерийінің бит орындарына сәйкес өзгеру ықтималдығы

бульдік функцияларға негізделген S-блоктардың құрылымы жайлы ең алғаш Адамс пен С. Таварес, Квангжо Ким еңбектерінде зерттелді. Бульдік функцияның қатаң лавиндік критерийін зерттеу келесі белгілеулер, ұғымдар мен анықтамаларға негізделген [18].

Бізде F_2^n – n өлшемді екілік векторлық кеңістік болсын және мұндағы $F_2 - \{0,1\}$ элементтерінен тұратын Галуа өрісі болсын. n және m - натурал сандар болсын, онда векторлы бульдік функция F-ті мына түрде анықтаймыз: $F : F_2^n \mapsto F_2^m$.

1-анықтама. $F(x) = (f_1, f_2, \ldots, f_m)$ функциясындағы $f_1, f_2, \ldots, f_m$ – бульдік функциялары F бульдік функцияның координаталары деп аталады. $m = 1$ кезінде векторлы бульдік функция шығысында тек бір бит ғана болатын кәдімгі бульдік функцияға эквивалентті.

2-анықтама. $f(x) : F_2^n \mapsto F_2$ – n айнымалысы бар бульдік функция болсын, мұндағы $x = (x_0, x_1, \ldots, x_{n-1})$. Онда $f(x)$ функциясының хемминг салмағы былай анықталады:

$$hw(f) = \sum_{x=0}^{2^n-1} f(x). \tag{4}$$

3-анықтама. $f(x): F_2^n \mapsto F_2$ бульді функциясы болсын. Онда $f(x)$ функциясының $u \in F_2^n$ екілік векторы арқылы алынған өсімшесі былай анықталады:

$$D_u f(x) = f(x) \oplus f(x+u). \tag{5}$$

4-анықтама. Қандай да бір бульдік функция $f(x)$ қатаң лавиндік критерийді қанағаттандырады деп айтамыз, егер $u \in F_2^n$ үшін төмендегідей теңдеулер жүйесі орындалса:

$$\begin{cases} hw(u) = 1; \\ \sum_{x=0}^{2^n-1} (f(x) \oplus f(x+u)) = 2^{n-1}. \end{cases} \tag{6}$$

немесе ықтималдықтар түрінде былай жазуға болады:

$$\begin{cases} hw(u) = 1; \\ p\{f(x) = f(x+u)\} = 0.5. \end{cases} \tag{7}$$

Енді, негізгі жұмыс — S-блоктарға қатаң лавиндік критерийді тексеруге көшейік. Түсінікті болу үшін төрт "алтын" S-блоктың біріншісіне (S_1 -блок) жүргізілген талдауды толықтай қадамдап жүргізейік. S_1 -блокты декомпозиция арқылы бульдік функция компоненттерімен жазып алайық:

Кесте 3 – S_1 **-дің компоненттік жазбасы**

$S_1 =$	0	F	B	8	C	9	6	3	D	1	2	4	A	7	5	E
1-жол	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0
2-жол	0	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1
3-жол	0	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1
4-жол	0	1	1	1	1	1	0	0	1	0	0	0	1	0	0	1

Бұдан әрі, Кесте-3-тен біз S-box бірінші жолдың компоненттік мәндері негізінде төрт айнымалысы бар $(n = 4)$ бульдік функциясын қатаң лавиндік критерийіне сәйкестігін зерттеуге көшеміз:

$$f_1(x_1, x_2, x_3, x_4) = \{0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0\}. \tag{8}$$

Бұдан әрі 3-ші және 4-анықтамаға сүйене отырып, келесі кестені құрайық. Бұл Кесте-4-те $f_1(x)$ бульдік функцияның төрт айнымалысының барлық мүмкін мәндеріндегі (8)-өрнекке сәйкес нәтижелері, $f_1(x)$ бульдік функцияның $hw(u) = 1$ өсімшесімен қосылған аргументіндегі мәні және $D_u f_1(x)$ (Кестеде D_u деп белгіленген) өсімшесінің нәтижелері көрсетілген.

Енді, Кесте-3-ті пайдаланып, осындай есептеулерді біз S_1 -блоктың 2-ші, 3-ші және 4-ші жолдарының компоненттік мәндері:

$$\begin{gathered} f_2(x_1, x_2, x_3, x_4) = \{0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1\}, \\ f_3(x_1, x_2, x_3, x_4) = \{0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1\}, \\ f_4(x_1, x_2, x_3, x_4) = \{0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1\} \end{gathered}$$

үшін жүргіземіз. Соңында, S_1 -блоктың барлық жолдарының компоненттері арқылы алынған нәтижелер төмендегідей матрица түрінде өрнектейік:

$$SAC_{S_1} = \begin{pmatrix} \Sigma D_{0001} f_1(x) & \Sigma D_{0010} f_1(x) & \Sigma D_{0100} f_1(x) & \Sigma D_{1000} f_1(x) \\ \Sigma D_{0001} f_2(x) & \Sigma D_{0010} f_2(x) & \Sigma D_{0100} f_2(x) & \Sigma D_{1000} f_2(x) \\ \Sigma D_{0001} f_3(x) & \Sigma D_{0010} f_3(x) & \Sigma D_{0100} f_3(x) & \Sigma D_{1000} f_3(x) \\ \Sigma D_{0001} f_4(x) & \Sigma D_{0010} f_4(x) & \Sigma D_{0100} f_4(x) & \Sigma D_{1000} f_4(x) \end{pmatrix} = \begin{pmatrix} 12 & 12 & 8 & 8 \\ 8 & 12 & 12 & 8 \\ 12 & 8 & 12 & 12 \\ 8 & 12 & 8 & 12 \end{pmatrix}. \tag{9}$$

Кесте 4 – берілген $f(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_1(x)$	$f_1(x \oplus 0001)$	D_{0001}	$f_1(x \oplus 0010)$	D_{0010}	$f_1(x \oplus 0100)$	D_{0100}	$f_1(x \oplus 1000)$	D_{1000}
$f(0000)=0$	$f(0001)=1$	1	$f(0010)=1$	1	$f(0100)=0$	0	$f(1000)=1$	1
$f(0001)=1$	$f(0000)=0$	1	$f(0011)=0$	1	$f(0101)=1$	0	$f(1001)=1$	0
$f(0010)=1$	$f(0011)=0$	1	$f(0000)=0$	1	$f(0110)=0$	1	$f(1010)=0$	1
$f(0011)=0$	$f(0010)=1$	1	$f(0001)=1$	1	$f(0111)=1$	1	$f(1011)=0$	0
$f(0100)=0$	$f(0101)=1$	1	$f(0110)=0$	0	$f(0000)=0$	0	$f(1100)=0$	0
$f(0101)=1$	$f(0100)=0$	1	$f(0111)=1$	0	$f(0001)=1$	0	$f(1101)=1$	0
$f(0110)=0$	$f(0111)=1$	1	$f(0100)=0$	0	$f(0010)=1$	1	$f(1110)=1$	1
$f(0111)=1$	$f(0110)=0$	1	$f(0101)=1$	0	$f(0011)=0$	1	$f(1111)=0$	1
$f(1000)=1$	$f(1001)=1$	0	$f(1010)=0$	1	$f(1100)=0$	1	$f(0000)=0$	1
$f(1001)=1$	$f(1000)=1$	0	$f(1011)=0$	1	$f(1101)=1$	0	$f(0001)=1$	0
$f(1010)=0$	$f(1011)=0$	0	$f(1000)=1$	1	$f(1110)=1$	1	$f(0010)=1$	1
$f(1011)=0$	$f(1010)=0$	0	$f(1001)=1$	1	$f(1111)=0$	0	$f(0011)=0$	0
$f(1100)=0$	$f(1101)=1$	1	$f(1110)=1$	1	$f(1000)=1$	1	$f(0100)=0$	0
$f(1101)=1$	$f(1100)=0$	1	$f(1111)=0$	1	$f(1001)=1$	0	$f(0101)=1$	0
$f(1110)=1$	$f(1111)=0$	1	$f(1100)=0$	1	$f(1010)=0$	1	$f(0110)=0$	1
$f(1111)=0$	$f(1110)=1$	1	$f(1101)=1$	1	$f(1011)=0$	0	$f(0111)=1$	1
		Σ=12		Σ=12		Σ=8		$\Sigma=8$

Дәл осындай есептеу жолымен біз қолданған S_2-блок, S_3-блок және S_4-блок үшін төмендегідей нәтижелер аламыз:

$$SAC_{S_2}=\begin{pmatrix}8&12&12&8\\12&8&12&8\\12&8&12&8\\12&12&8&12\end{pmatrix}, SAC_{S_3}=\begin{pmatrix}12&8&12&8\\8&12&12&8\\8&12&12&8\\12&8&8&12\end{pmatrix}, SAC_{S_4}=\begin{pmatrix}12&12&8&8\\12&8&8&12\\8&12&12&12\\8&12&8&12\end{pmatrix}. \tag{10}$$

(6)-формулаға сүйенсек, алынған мәндер оң нәтиже беру үшін олар $N/2=8$ саны маңында болуы тиіс, мұндағы $N=2^4$. (9) бен (10)-нан байқайтынымыз, таңдап алынған S-блок алмастырулар қатаң лавиндік эффектіні (SAC) орта есеппен 70-75% қанағаттандырады, яғни оларды шифрлау алгоритмінің тиімді примитиві ретінде қолдануға болады. Дегенмен, тәжірибеде SAC-ті 100% қанағаттандыратын кейбір S-блоктар дифференциалдық талдауға төзімсіздік танытып жатады: мысалы дереккөз [17]-де қарастырылған S-блок – $S=\{4,7,2,14,1,13,8,11,15,12,6,10,5,9,3,0\}$. Сол себепті, алдағы уақытта қарастырып отырған S-блоктарға дифференциалды және сызықты талдау, олардың векторлық бульдік функциялар арқылы жазбасындағы сызықсыздық дәрежесін, қасиеттерін және коррелациялық, алгебралық, статистикалық талдаулар негізіндегі шабуылдарға төзімділігін анықтау бағытында зерттеулер жүргізу қажеттілігі туындады.

2.3.3. CF шифрлау алгоритмінің қатаң лавиндік эффектін зерттеу

Шифрлау алгоритмінің қатаң лавиндік критерийі

$$\varepsilon_s=|2*k_{si,j}-1| \tag{11}$$

арқылы бағаланады, мұндағы i – шифрлаудың кіріс мәндегі өзгертілген биттің нөмірі, j – шифрлаудың шығыс мәніндегі талданатын биттің нөмірі, $k_{si,j}$ – j–ші шығыс биттің өзгертілген i-ші кіріс битке қатысты өзгеруінің ықтималдығы. Яғни, бұл критерий лавиндік критерийге қарағанда талапты жоғары қояды: өзгертілген әрбір кіріс битіне байланысты әрбір шығыс битінің өзгеру қасиетін қарастырады. Теорияда бұл өзгерістің ықтималдығы 0,5-ке жуықтау болуы қажет.

Тәжірибеде талдауымызды мына бағытта жүргіземіз. Алдымен P_0^k ашық мәтінді толық 4 раундпен шифрлаймыз, нәтижені C_0^k деп белгілейік, мұндағы k – ашық мәтіндер нөмірі. Талдау үшін ашық мәтіннің әрбір кіріс i–битін инверсиялап, оны P_i^k ретінде

қарастырып, шифрлау арқылы соған сәйкес C_i^k шифрмәтінін алып отырамыз, мұнда $i = 1, \ldots, 128$. Әрбір P_i^k үшін C_i^k шифрмәтіндегі j–ші битті бастапқы C_0^k шифрмәтіндегі j–ші битімен салыстыратын боламыз, мұндағы $j = 1, \ldots, 128$. Бізге салыстыру нәтижелеріне талдау жүргізу үшін төмендегідей 128x128 өлшемдегі Q^k матрицасы қажет болады:

$$Q^k = \begin{pmatrix} q_{1,1}^k & q_{1,2}^k & \cdots & q_{1,128}^k \\ q_{2,1}^k & q_{2,2}^k & \cdots & q_{2,128}^k \\ \cdots & \cdots & \cdots & \cdots \\ q_{128,1}^k & q_{128,2}^k & \cdots & q_{128,128}^k \end{pmatrix}. \tag{12}$$

Мұнда, $q_{i,j}^k$ – P_0^k ашық мәтіннің i–битін инверсиялап, шифрлау жүргізгенде алынған C_i^k шифрмәтіннің j–ші битінің C_0^k шифрмәтіндегі j–ші битімен салыстыратын өзгеруі, яғни

$$q_{i,j}^k = \begin{cases} 1, & \text{салыстыруда өзгеріс болса;} \\ 0, & \text{салыстыруда өзгеріс болмаса.} \end{cases} \tag{13}$$

Қатаң лавиндік критерийдің орындалуын эмипирикалық түрде тексеру үшін біз әртүрлі екі жүз P_0^k ашық мәтін алдық, $k = 1, 2, \ldots, 200$. Әр k үшін жоғарғы процесті жүргізіп, сәйкесінше екі жүз Q^k алатын боламыз. Алынған екі жүз Q^k матрицасының k бойынша сәйкес элементтерінің қосындысын шығарып, оны төмендегідей белгілейік:

$$R = \begin{pmatrix} \sum_{k=1}^{200} q_{1,1}^k & \sum_{k=1}^{200} q_{1,2}^k & \cdots & \sum_{k=1}^{200} q_{1,128}^k \\ \sum_{k=1}^{200} q_{1,1}^k & \sum_{k=1}^{200} q_{1,2}^k & \cdots & \sum_{k=1}^{200} q_{1,128}^k \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{k=1}^{200} q_{128,1}^k & \sum_{k=1}^{200} q_{128,2}^k & \cdots & \sum_{k=1}^{200} q_{128,128}^k \end{pmatrix}. \tag{14}$$

Бұдан әрі, $p_{si,j}$ ықтималдығын алу үшін R матрицасының әр элементін ашық мәтіндер санына - 200-ге бөлеміз, сонда:

$$Pr_s = \begin{pmatrix} p_{s1,1} & p_{s1,2} & \cdots & p_{s1,128} \\ p_{s2,1} & p_{s2,2} & \cdots & p_{s2,128} \\ \cdots & \cdots & \cdots & \cdots \\ p_{s128,1} & p_{s128,2} & \cdots & p_{s128,128} \end{pmatrix}. \tag{15}$$

Алынған $p_{si,j}$ негізінде (11) формула арқылы CF шифрлау алгоритмінің қатаң лавиндік критерийін қанағаттандыруын бағалайтын боламыз, мұндағы $i, j = 1, \ldots, 128$. Бұл есептеулерді жүргізу үшін "Ақпараттық қауіпсіздік" зертханасында арнайы компьютерлік бағдарлама әзірленді. Бағдарлама көмегімен таңдап алынған 200 ашық мәтінге қатаң лавиндік критерийін анықтау мақсатында төмендегідей ықтималдықтар матрицасын алдық:

$$Pr_s = \begin{pmatrix} 0,56 & 0,50 & 0,51 & 0,54 & 0,53 & 0,46 & ... & 0,53 \\ 0,52 & 0,50 & 0,50 & 0,49 & 0,49 & 0,47 & ... & 0,47 \\ 0,49 & 0,41 & 0,42 & 0,47 & 0,53 & 0,51 & ... & 0,57 \\ 0,47 & \mathbf{0,45} & 0,44 & 0,52 & 0,50 & 0,55 & ... & 0,51 \\ 0,49 & 0,51 & 0,49 & 0,47 & 0,51 & 0,45 & ... & 0,53 \\ 0,55 & 0,59 & 0,47 & 0,48 & 0,51 & 0,49 & ... & 0,53 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0,45 & 0,56 & 0,54 & 0,47 & 0,51 & 0,61 & ... & 0,51 \end{pmatrix}. \tag{16}$$

Мысалы, 200 ашық мәтіннің әрбір 4–ші битін инвертациялап шифрлағанда, 200 шифрмәтіннің әрқайсының 2–ші битінің бастапқы инвертацияланбаған нұсқасынан өзгеру ықтималдығы тәжірибе жүзінде 0,45–ке тең болды.

(11) формула көмегімен төмендегі 5–кестеде көрсетілген ε_s қатаң лавиндік параметрдің статистикалық көрсеткіштерін алдық.

CF шифрлау алгоритмінің қатаң лавиндік критерийін талдауы бойынша қорыта келгенде, 5-кестедегі мәндер теориялық тұрғыдан алғанда оң нәтижелер көрсетеді. Осы нәтижелер көрсеткендей, шифрлаудың кірісіндегі әрбір i–ші биттің өзгерісі шифрмәтіннің

Кесте 5 – ε_s **қатаң лавиндік параметрдің статистикалық көрсеткіштері**

	Pr_s ықтималдығы	ε_s–нің мәндері
Максимальды мән	0,6562	0,3125
Минималді мән	0,3437	0
Арифметикалық орта мән	0,5004	0,0710
Дисперсия	0,0018	0,0027
Мода	0,5078	0,0156
Медиана	0,5000	0,0625

j –ші битінің өзгерісін 0,5 ықтималдықтен туындатады. Осы себепті аталған алгоритм қатаң лавиндік критерийін толық қанағаттандырады.

2.3.4. Шифрлау алгоритмінің тиімді раундтар санын анықтау

Қарастырылған шифрлау алгоритміне жүргізілген лавиндік және қатаң лавиндік критерийлердің сараптамаларын бағалау нәтижесінде бойынша раундтар санының төменгі мәні 4 ретінде қарастыру жеткілікті. Раунд санының ең тиімді мәнін таңдап алу мақсатында төмендегідей фактілерді ескерген жөн.

Алгоритм жұмыс істеу сұлбасында көрсетілгендей, бір раунд ішінде S-блок алмастыруы екі рет жүргізіледі, яғни Stage-1 және Stage-3 түрлендіруінде. Айта кететін жайт, осы екі түрлендірулерде сызықты (xor) және сызықты емес операциялар әр байтты есептеу барысында кезектесіп орындалып отырады. Бұл өз кезегінде диффузиялық қасиеттің жоғарғы деңгейге жетуіне әкеледі. Оның дәлелі ретінде 1-раундтан кейінгі биттік шашырау нәтижесінен көруге болады.

Төменгі Кесте-6–да ε_α лавиндік параметрінің 1, 2, 4, 8, 12–раундтардан кейінгі статистикалық көрсеткіштері көрсетілген. Осы кестеден байқайтынымыз, 1–ші және 2–раундтарда статистикалық көрсеткіштер қалған раундтар көрсеткіштеріне қарағанда нашарлау, ал 4–раундтан бастап әрі қарай раунд ұлғайған сайын да мәндер бір-бірлерімен шамалас болып отыр.

Алынған лавиндік эффект нәтижелерінің қорытындысы бойынша раундтар саны әзірше 4–ке тең болуы жеткілікті болды. Алайда, дифференциалды, сызықты, алгебралық және де басқа заманауи криптоталдау әдістеріне төтеп беру үшін, сондай-ақ кілттердің әрбір биті шифрмәтіннің әрбір битіне әсер ету мәселесі, шығатын биттердің бір-біріне тәуелсіздік мәселесі сияқты тағы да басқа маңызды мәселелер раунд санының артуына алып келуі мүмкін, осы бағытта алдағы уақытта зерттеулер жүргізу талап етіледі.

Кесте 6 – ε_α **лавиндік параметрдің статистикалық көрсеткіштері**

ε_α статистикалық көрсеткіштері	1–раунд	2–раунд	**4–раунд**	8–раунд	12–раунд
Максимальды мән	0,2814	0,3437	**0,2400**	0,2342	0,2343
Минималді мән	0	0	**0**	0	0
Арифметикалық орта мән	0,0743	0,0711	**0,0668**	0,0702	0,0713
Дисперсия	0,0026	0,0037	**0,0022**	0,0029	0,0029
Мода	0,0625	0	**0,0460**	0	0,0468
Медиана	0,0625	0,047	**0,0500**	0,0425	0,0625

2.3.5. CFKey раундтық кілттерді жасау алгоритмін талдау

Қарастырылған CFKey алгоритмінде бастапқы құпия кілт арқылы бізге қажетті жасалынатын төрт раундтық кілттердің қауіпсіздік дәрежесін анықтайық. Осы мақсатта бастапқы кілттің әрбір битінің өзгерісі CF шифрлау алгоритмі арқылы алынған шифрмәтінді қаншалықты деңгейде өзгеріске ұшырататыны бағытында зерттеу жұмысы жүргізілді. Басқа сөзбен айтқанда, шифрмәтіннің бастапқы кілтке қатысты "лавиндік эффекті" тексерілді. Ол үшін 128 биттік ұзындықтағы бастапқы кілт ретінде

0xCC156C4CE0024D5113D680D7CCE6D8B2 кездейсоқ таңдап алдық. Осы кілттің әрбір битін кезектеп инверсиялап, қосымша 128 бастапқы кілт алдық. Әрі қарай, 129 кілт арқылы кездейсоқ таңдалған "Alga_Kazakhstan!" ашық мәтінін шифрлап, сәйкес 129 шифрмәтін алдық. Осылайша, нәтижелерді талдап, CFKey алгоритмі арқылы жасалған раундтық кілттердің "лавиндік критерийді" қанағаттандыратынына көз жеткізейік.Сурет-7-ден әрбір 1-ден 128-ге дейінгі жеке-жеке өзгерген биттер үшін шифрмәтіннің жалпы мәндерінің өзгеру ықтималдығын көруге болады. Кесте-7-де арнайы бағдарлама

Кесте 7 – Кілттің ε_α лавиндік параметрге әсері

i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α
1	0,05	17	0,16	33	0,03	49	0,14	65	0,11	81	0,05	97	0,02	113	0,14
2	0,13	18	0,03	34	0,05	50	0,03	66	0,03	82	0,17	98	0,09	114	0,08
3	0,02	19	0,11	35	0,09	51	0,08	67	0,02	83	0,16	99	0,03	115	0,06
4	0,02	20	0,13	36	0,02	52	0,00	68	0,09	84	0,06	100	0,05	116	0,13
5	0,03	21	0,06	37	0,08	53	0,03	69	0,03	85	0,22	101	0,03	117	0,11
6	0,08	22	0,09	38	0,11	54	0,05	70	0,13	86	0,02	102	0,00	118	0,11
7	0,05	23	0,03	39	0,05	55	0,14	71	0,02	87	0,03	103	0,02	119	0,03
8	0,09	24	0,03	40	0,19	56	0,00	72	0,03	88	0,05	104	0,14	120	0,06
9	0,08	25	0,02	41	0,09	57	0,03	73	0,09	89	0,03	105	0,06	121	0,06
10	0,09	26	0,13	42	0,08	58	0,11	74	0,03	90	0,05	106	0,03	122	0,02
11	0,05	27	0,08	43	0,02	59	0,02	75	0,03	91	0,11	107	0,02	123	0,00
12	0,02	28	0,16	44	0,05	60	0,00	76	0,19	92	0,00	108	0,05	124	0,03
13	0,03	29	0,13	45	0,02	61	0,11	77	0,06	93	0,09	109	0,11	125	0,22
14	0,11	30	0,05	46	0,06	62	0,05	78	0,05	94	0,09	110	0,17	126	0,02
15	0,02	31	0,13	47	0,02	63	0,02	79	0,05	95	0,11	111	0,09	127	0,02
16	0,20	32	0,02	48	0,13	64	0,11	80	0,11	96	0,23	112	0,16	128	0,11

арқылы алынған 128 шифрмәтіннің ε_α лавиндік әсері параметрінің әрбір өзгерген бит орындарындағы мәндері, ал кесте-8-де осы мәндердің статистикалық көрсеткіштері көрсетілген.

Кесте 8 – ε_α лавиндік параметрдің статистикалық көрсеткіштері

Минималді мән	Максимальды мән	Арифметикалық орта мән	Дисперсия
0	0,23	0,07	0,002

Сурет 7 – Биттік шашырау критерийінің бит орындарына сәйкес өзгеру ықтималдығы

Кесте-7 мен Кесте-8 және Сурет-7-ден мынандай қортынды шығаруға болады:

кездейсоқ алынған бастапқы құпия кілттен алынатын раундтық кілттердің негізінде алынған шифрмәтін осы бастапқы кілттің әрбір битінің өзгерісіне 0,5 ықтималдықтен тәуелді. Яғни, бастапқы кілттің өте аз өзгерісі шифрмәтіннің биттерін 50 пайыздық өзгеріске ұшыратады. Бұл қасиет CFKey алгоритмі раундтық кілттерге қойылатын талаптарға сай екендігін көрсетеді. CF алгоритміндегі мынандай ерекшелік бар: оның құрамындағы SBOX процедурасы арқылы бірдей мәндерден тұратын ашық мәтін мәндердің орналасу орнына байланысты белгілі тәртіппен S-блоктан өткенде, әртүрлі шығыс мәтіндер беретін болады. Мысалы, 16 байттан тұратын құпия кілт былай алынсын: $(32, 32, 32, 32, \ldots, 32)_{16}$, сонда келесідегідей бір-бірінен өзгеше шығыс мәндер аламыз:

$$A = \begin{pmatrix} 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \end{pmatrix} \overset{SBOX}{\rightarrow} \begin{pmatrix} B8 & E8 & F8 & 38 \\ B1 & E1 & F1 & 31 \\ B5 & E5 & F5 & 35 \\ B4 & E4 & F4 & 34 \end{pmatrix}. \tag{17}$$

Бұның сыртында StageKey-1 және StageKey-3 түрлендірулерінде матрицаның әр элементін есептегенде, xor операциясы мен S-блоктан өткізу операциясы кезектесіп орындалатынын есепке алатын болсақ, "осал кілттер" классы тарыла түседі.

3. Қорытынды

Бұл мақалада блоктық шифлау алгоритмдерінің негізгі талаптары мен ұсыныстарын қанағаттандыратын жаңа CF симметриялық блокты шифрлау алгоритмі құрылымы, оның кілт жасау алгоритмі, бағдарламалық жүзеге асырылуы және "лавиндік эффект" қасиеті мен "қатаң лавиндік эффект" қасиеті көрсетілген. Алгоритмнің құрамындағы сызықты және сызықты емес түрлендіру әдістеріне жеке-жеке тоқталып, алгоритмнің жұмыс құрылымы түсіндірілді. Сонымен бірге, жұмыс істеу өнімділігі талданып, оның жылдамдығы жағынан жақсы көрсеткіш көрсеткені анықталған, яғни бағдарлама көмегімен әр түрлі өлшемдегі, кеңейтуі әртүрлі файлдарды алып шифрлап, шифрлау жылдамдығы жылдам жасайтындығы анықталды. Алгоритмның биттік шашырату критерийі 1-ші раундтан кейін-ақ қажетті деңгейде екені көрсетілді. CF шифрлау алгоритмінің қатаң лавиндік критерийін талдауы қорытындысы бойынша да оң нәтижелер алынды. Жұмыс барысында қолданылатын төрт S-блоктардың қатаң лавиндік критерийін қанағаттандыруы тексерілді. Алайда, қажетті мөлшердегі раунд саны әзірше – 4, ол алдағы уақытта криптоберіктілікті талдау барысында жұмыс өнімділігін ескере отырып, әлі де нақтыланатын болады. Қазіргі уақытта алгоритмнің криптоберіктілігін статистикалық және алгебралық тәсілдермен талдау жұмыстары жүргізуде.

4. Алғыс

Жұмыс OR11465439 "Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хэштеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау" бағдарламалық-нысаналық қаржыландыру ғылыми жобасы аясында жүргізілді.

Әдебиеттер тізімі

1 Столлингс В. Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. - Москва: Вильямс, 2001. -672 с.

2 Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - Москва: Гелиос АРВ, 2006. - 376 с.

3 Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Конечные поля. - Москва: КУДИЦ-ОБРАЗ, 2002. - 176 с.

4 Панасенко С.П. Алгоритмы шифрования. Специальный справочник. -СПб.: БХВ-Петербург, 2009. - 576 с.

5 Д.С. Дюсенбаев, К.Т. Алғазы, Қ.С. Сақан. Симметриялы шифрларда қолданылатын сызықты емес түйіндерді зерттеу // Матер. межд. науч.-практ. конф. "Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020". - Алматы, 2020. - Б.34-39.

6 Aboushosha B., Ramadan R.A., Dwivedi A.D., El-Sayed A. and Dessouky M.M. SLIM: "A Lightweight Block Cipher for Internet of Health Things", in IEEE Access. -2020. -Vol. 8. -P. 203747-203757. -doi: 10.1109/ACCESS.2020.3036589. (01.09.2021).
7 Ghosha A., Sadhukhan R., Patranabis S., Datta N., Picek S., Mukhopadhyay D. Lightweight and Side-channel Secure 4x4 S-Boxes from Cellular Automata Rules// IACR Transactions on Symmetric Cryptology. -2018. 3. P. 311-334. https://doi.org/10.13154/tosc.v2018.i3.311-334. (21.08.2021).
8 Hicks C., Garcia F. D., Oswald D. Dismantling the AUT64 Automotive Cipher// IACR Transactions on Cryptographic Hardware and Embedded Systems. -2018(2). -P. 46-69. URL: https://doi.org/10.13154/tches.v2018.i2.46-69. (02.10.2021).
9 Jiqiang Lu, Hwajung Seo A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design// Security and Communication Networks. -2020. Vol. 2020. 1-26 pages, URL: https://doi.org/10.1155/2020/1457419. (21.07.2021).
10 Горбенко И.Д., Долгов И.В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И. Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования // Известия ЮФУ. Технические науки. -2007. №1. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.03.2021).
11 Saarinen, Markku-Juhani O. Cryptographic Analysis of All 4 x 4 - Bit S-Boxes// Selected Areas in Cryptography. SAC 2011. Lecture Notes in Computer Science. -2012. -vol 7118. pp. 118-133, Springer, Berlin, Heidelberg. $https://doi.org/10.1007/978-3-642-28496-0_7$
12 Anderson R., Biham E. and Knudsen L. Serpent: A Proposal for the Advanced Encryption Standard// NIST AES Proposal, 1998, pp. 1-23. Available at: http://www.cl.cam.ac.uk/ rja14/Papers/serpent.pdf (1999) (14.09.2021).
13 Engels D., Fan X., Gong G., Hu H. and Smith E. M. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices// In R. Sion et al. (Eds.): FC 2010 Workshops, LNCS 6054, -P. 3-18. Springer.
14 Engels D., Saarinen M.-J. O., Schweitzer P. and Smith E. M. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm//RFIDSec 2011, The 7th Workshop on RFID Security and Privacy, 26-28 June 2011, Amherst, Massachusetts, USA (2011).
15 Vergili I., Y?cel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen? S-Boxes // Turk J Elec Engin. - 2001. - T. 9, № 2. - P. 137-145.
16 Levinskas Matas, Mihalkovich Aleksejus Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power// Mathematical Models in Engineering. -2021. -Vol. 7. -Issue 3. -P. 50-53. URL: https://doi.org/10.21595/mme.2021.22234. (10.08.2021).
17 Сейткулов, Е., Оспанов, Р., Ергалиева, Б. On cryptographic properties of S-boxes// VESTNIK KAZNRTU. -2021. -Vol. 143. No 4. -P. 96-103. URL: https://doi.org/10.51301/vest.su.2021.i4.12.
18 Sokolov A., Zhdanov O. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength// Siberian Journal of Science and Technology. -2019. 20. -P. 183-190.

С.Е.Нысанбаева [1,2] , К.Т. Алгазы [1] , Қ.С.Сакан [1,2] , А.Хомпыш [1,2] , Д.С.Дуйсенбаев [1]

[1] *Институт информационных и вычислительных технологий, г. Алматы, Казахстан*
[2] *Казахский национальный университет им. аль-Фараби, г.Алматы, Казахстан*

Блочный алгоритм шифрования CF и исследование его критерий лавинного эффекта

Аннотация: В статье описываются значимость, особенность и область применения симметричных блочных шифров, используемых для обеспечения конфиденциальности данных в процессе развития современных вычислительных технологий. Кратко изложена структура алгоритма шифрования "CF" и механизм генерации раундовых ключей на основе основного ключа симметричного блока, разработанного в Лаборатории информационной безопасности Института информационных и вычислительных технологий. Разработана программная реализация созданного алгоритма шифрования, на основе которого проверены производительность работы и битовое рассеивание (свойство "лавинного эффекта" и свойство "строгого лавинного эффекта") между открытым текстом и соответствующим ему шифртекстом. С целью оптимизации аппаратной реализации алгоритма применено преобразование S-блока замены, рассматриваемое как нелинейный узел, размером 4x4 бит.

Ключевые слова: алгоритмы шифрования, криптостойкость алгоритма, критерий "лавинного эффекта", критерий "строгого лавинного эффекта".

S.E.Nyssanbayeva [1,2] , K.Algazy [1] , K.S.Sakan [1,2] , A. Khompysh [1,2] , D.S.Dyussenbayev [1]

[1] *Institute of Information and Computing Technologies, Almaty, Kazakhstan*
[2] *al-Farabi Kazakh National University, Almaty, Kazakhstan*

The encryption algorithm "FC" and analysis of its avalanche effect criterion

Abstract: The article is about the importance, features and scope of symmetric block ciphers used to ensure the confidentiality of data in the era of rapid development of modern computing technologies. In this paper, the structure of the symmetric block encryption algorithm CF, developed in the "Laboratory of Information Security" of the "Institute of Information and Computational Technologies", the round keys generating mechanism based on it's secret key are described.

A computer program of the created encryption algorithm was developed, on the basis of which the performance was studied and the bit scattering between the plaintext and the ciphertext (the property of the "avalanche effect" and "strong avalanche effect") was checked. In order to optimize the hardware implementation of the algorithm, the conversion of the S-block, which is considered as a nonlinear node, was obtained in 4x4 bit size.

Keywords: encryption algorithm, cryptographic strength, avalanche effect, strong avalanche effect.

References

1 Stalling W. Kriptografiya i zashchita setej: principy i praktika [Cryptography and Network Security: Principles and Practice]. Second Edition. Trans. from eng. (Williams, Moscow, 2001, 672 p.).

2 Babenko L.K., Ishchukova E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ih analiza [Modern block encryption algorithms and methods of their analysis]. (Helios, Moscow, 2006. 376 p.).

3 Zenzin O.S., Ivanov M.A. Standart kriptograficheskoj zashchity - AES [AES - Cryptographic Security Standard]. Finite field. (KUDITS-OBRAZ, Moscow, 2002. 176 p.).

4 Panasenko S.P. Algoritmy shifrovaniya. Special'nyj spravochnik. [Encryption algorithms. A special reference book] (bhv, Saint Petersburg, 2009, 576 p.).

5 Dyusenbaev D.S., Algazy K.T., Sakan K.S. Simmetriyalyi shifrlarda koldanyilatyin sizyiktyi emes tuinderdi zertteu [Study of nonlinear nodes used in symmetric ciphers], Mater. of Int. Sci.-pract. Conf. " Actual problems of information security in Kazakhstan APIBK-2020". Almaty, 2020. 34-39.

6 Aboushosha B., Ramadan R.A., Dwivedi A.D., El-Sayed A. and Dessouky M. M. SLIM: A Lightweight Block Cipher for Internet of Health Things, in IEEE Access. Vol. 8, P. 203747-203757, 2020, doi: 10.1109/ACCESS.2020.3036589. (01.09.2021).

7 Ghoshal A., Sadhukhan R., Patranabis S., Datta N., Picek S., Mukhopadhyay D. Lightweight and Side-channel Secure 4x4 S-Boxes from Cellular Automata Rules. IACR Transactions on Symmetric Cryptology, 2018(3), 311-334. https://doi.org/10.13154/tosc.v2018.i3.311-334. (21.08.2021).

8 Hicks C., Garcia F.D., Oswald D. Dismantling the AUT64 Automotive Cipher. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(2), 46-69. Available at: https://doi.org/10.13154/tches.v2018.i2.46-69. (02.10.2021).

9 Jiqiang Lu, Hwajung Seo A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design, Security and Communication Networks, 2020, Vol. 2020, 1-26 pages, 2020. Available at: https://doi.org/10.1155/2020/1457419. (21.07.2021).

10 Gorbenko I.D., Dolgov I.V., Oleynikov R.V., Rujentsev V.I., Mihaylenko M.S., Gorbenko YU.I. Razrabotka trebovaniy i printsip proektirovaniya perspektivnogo simmetrichnogo blochnogo algoritma shifrovaniya [Development of requirements and the design principle of a promising symmetric block encryption algorithm]// Izvestiya SFedU. Engineering sciences. 2007. №1. Available at: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.03.2021).

11 Saarinen, Markku-Juhani O. Cryptographic Analysis of All 4 x 4 - Bit S-Boxes, Selected Areas in Cryptography. SAC 2011. Lecture Notes in Computer Science, vol 7118, 2012, pp. 118-133, Springer, Berlin, Heidelberg. $https://doi.org/10.1007/978-3-642-28496-0_7$

12 Anderson R. , Biham E. and Knudsen L. Serpent: A Proposal for the Advanced Encryption Standard, NIST AES Proposal, 1998, pp. 1-23. Available at: http://www.cl.cam.ac.uk/ rja14/Papers/serpent.pdf (1999) (14.09.2021).

13 Engels D., Fan X., Gong G., Hu H. and Smith E.M. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices, In R. Sion et al. (Eds.): FC 2010 Workshops, LNCS 6054, pp. 3-18. Springer.

14 Engels D., Saarinen M.-J. O., Schweitzer P., and Smith E. M. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm, RFIDSec 2011, The 7th Workshop on RFID Security and Privacy, 26-28 June 2011, Amherst, Massachusetts, USA (2011).

15 Vergili I., Y?cel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen? S-Boxes, Turk J Elec Engin, 9(2), 137-145(2001).

16 Levinskas Matas, Mihalkovich Aleksejus Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power, Mathematical Models in Engineering, 7(3), 50-53(2021). Available at: https://doi.org/10.21595/mme.2021.22234. (10.08.2021).

17 Seitkulov Y.N., Ospanov R.M., Yergaliyeva B.B. On cryptographic properties of S-boxes, VESTNIK KAZNRTU, 143(4), 96-103(2021). Available at: https://doi.org/10.51301/vest.su.2021.i4.12.

18 Sokolov A., Zhdanov O. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength, Siberian Journal of Science and Technology. 20. 183-190(2019). 10.31772/2587-6066-2019-20-2-183-190.

Авторлар туралы мағлұмат:

Нысанбаева С.Е. – т.ғ.д., қауымд. профессор, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының бас ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Алгазы К.Т. – Phd, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Сақан К.С – ***корреспонденция үшін автор***, әл-Фараби атындағы ҚазҰУ Phd докторанты, әл-Фараби даңғылы, 71 үй, 050040, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Хомпыш А. – PhD, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Дүйсенбаев Д.С. – ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Nyssanbayeva S.E. – Dr.Tech.Sc., sassociate professor, Chief researcher of Information security laboratories, IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Algazy K.T. – PhD, researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Sakan K.S – ***correspondence author***, Phd student KazNU named after al-Farabi, 71 al-Farabi ave, 050040, Almaty, Kazakhstan. Researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Khompysh A. – PhD, researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Dyussenbayev D.S. - researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Поступила в редакцию 24.08.2021

Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2022, Vol. 138, №1, P.23-35
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

МРНТИ: **27.31.17, 30.19.33**

Л.А. Алексеева, Г.Д. Арепова

Институт математики и математического моделирования МОН РК, ул. Пушкина 125, Алматы, Казахстан
(E-mail: alexeeva@math.kz, arepovag@mail.ru)

Обобщенные решения краевых задач для уравнения Даламбера с локальными и связанными граничными условиями

Аннотация: Рассматриваются начально-краевые задачи для волнового уравнения с локальными и нелокальными линейными краевыми условиями на концах отрезка общего вида. Для их решения разработан метод обобщенных функций, который переводит исходные краевые задачи в решение волнового уравнения с сингулярной правой частью, содержащей сингулярные простые и двойные слои, плотности которых определяются граничными и начальными значениями искомой функции и ее производных. Получено интегральное представление решения через граничные функции, которые являются обобщением формулы Грина для решений волнового уравнения. Для определения неизвестных граничных функций построена в пространстве преобразований Фурье по времени разрешающая система из двух линейных алгебраических уравнений, которая связывает 4 граничные значения решения и его производных.Совместно с двумя краевыми условиями локального и нелокального типа построена разрешающая система уравнений для решения поставленных начально-краевых задач. На ее основе даны аналитические решения для классических трех краевых задач с условиями Дирихле, Неймана и смешанными на концах отрезка. Разработанный метод позволяет решать краевые задачи с различными локальными и нелокальными краевыми условиями и должен найти применение при решении волновых и других уравнений на графах различной структуры.

Кілт сөздер: уравнение Даламбера, краевая задача, начальные условия, краевые условия, метод обобщенных функций, функция Римана, обобщенное решение, разрешающие уравнения.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.2

2000 Mathematics Subject Classification: 35.

Введение

Решение многих задач акустики, гидромеханики, теории упругости и других разделов физики связано с решением краевых задач для гиперболических уравнений, описывающих процессы распространения волн в однородных изотропных средах. В последние десятилетия появилось много работ, посвященных дифференциальным уравнениям и краевым задачам на графах (в других терминах - пространственных сетях, одномерных стратифицированных множествах, одномерных клеточных комплексах) [1]. Краевые задачи на графах позволяют моделировать поведение самых разнообразных сетевых систем, как инженерно-технических, так и биологических, поэтому весьма актуально построение эффективных способов решения краевых задач для них с произвольной геометрией и разнообразным видом граничных условий и условий трансмиссии в узлах графа. Процессы передачи сигнала (возмущения, деформации и т.п.) по сетям описываются волновыми уравнениями,в частности, уравнением Даламбера. В работах [2-12] рассмотрен ряд краевых задач для этого уравнения на отрезке и на графах определенной структуры и вопросы их разрешимости. Отметим, что классическое

понятие дифференцируемости решений для гиперболических уравнений, каковым является уравнение Даламбера, резко сужает класс задач, полезных для приложений. В частности, типичные физические процессы, сопровождающиеся ударными волнами, не описываются дифференцируемыми решениями гиперболических уравнений. При применении численных методов решения для изучения таких процессов возникают сложности при построении разностных сеток и обеспечении точности выполнения граничных условий и условий на фронтах ударных волн, где производные функций терпят разрыв. Поэтому необходима разработка эффективных математических методов для исследования таких процессов.

Базовым элементом для волнового графа является отрезок конечной длины, на котором функция состояния графа удовлетворяет дифференциальному уравнению при разных краевых условиях на концах отрезка, которые могут быть и связанными. Здесь строятся решения начально-краевых задач для уравнения Даламбера на отрезке при локальных и нелокальных линейно-связанных краевых условиях. для решения задачи используется метод обобщенныых функций [12,13], который позволяет исследовать и ударные волны в таких системах. Этот метод позволяет перейти от поставленной начально-краевой задачи к решению уравнения Даламбера с сингулярной правой частью в пространстве обобщенных функций. При этом начальные и граничные условия входят в эти уравнения в виде плотности простых и двойных слоев правой части. Свертка ее с фундаментальным решением уравнения позволяет построить решение при известных граничных функциях и их производных. А асимптотические свойства решения - построить уравнения для определения неизвестных граничных функций. Для решения этих уравнений используется обобщенное преобразование Фурье. Получены разрешающие алгебраические уравнения для определения трансформант Фурье граничных функций, на основе которых построены решения ряда краевых задач в исходном пространстве-времени.

Разработанная методика построения решения волнового уравнения на отрезке позволяет строить линейные алгебраические системы разрешаюших уравнений на графах самой разнообразной структуры и исследовать периодические процессы в сетевых системах и нестационарные процессы, сопровождаемые ударными волнами.

1. Обобщенные решения волнового уравнения, ударные волны

Рассмотрим волновое уравнение Даламбера:

$$\Box_c u \equiv \frac{\partial^2 u}{\partial x^2} - c^{-2}\frac{\partial^2 u}{\partial t^2} = G(x,t), \tag{1}$$

где $G(x,t)$ – локально интегрируемая функция, c – положительная константа, которая, как известно, описывает скорость распространения волн в среде. Уравнение строго гиперболическое, класс его решений содержит разрывные по производным функции. Поверхности разрыва F – это характеристические поверхности, которые удовлетворяют характеристическому уравнению в $R^2 = \{(x, \tau = ct)\}$:

$$\nu_\tau^2 - \nu_x^2 = 0 \quad \Rightarrow \left|\frac{\nu_\tau}{\nu_x}\right| = 1. \tag{2}$$

Здесь (ν_x,ν_τ) - вектор нормали к F . Ему соответствуют характеристики: $x \pm ct = const$. В R^1 им соответствуют *волновые фронты* (F_t), движущиеся со скоростью c. На них выполняются условия Адамара:

$$[u(x,t)]_{F_t} = 0, \quad [u_{,t}]_{F_t} = -c\,[u_{,x}]_{F_t} \tag{3}$$

где через $[f(x,t)]_{F_t}$ обозначен скачок f на F_t :

$$[f(x,t)]_{F_t} = f^+(x,t) - f^-(x,t) = \lim_{\varepsilon\to+0}\left(f(x+\varepsilon,t) - f(x-\varepsilon,t)\right), \quad x \in F_t.$$

Класс подобных решений гиперболических уравнений называют *ударными волнами* , т.к. на их фронтах скорости испытывают скачки, вызванные скачком напряжений в физических средах.

Далее рассмотрим функции $u(x,t)$, которые непрерывны вместе с производными до второго порядка включительно почти всюду, за исключением конечного или счетного числа поверхностей разрыва - волновых фронтов, достаточно гладких почти всюду, на которых выполнены условия Адамара. Назовем такие решения *классическими.* Покажем, что они являются *обобщенными решениями* (1).

Для этого рассмотрим уравнение (1) на пространстве обобщенных функций медленного роста $S'(R^2) = \left\{\hat{f}(x,\tau)\right\}$ [15,16]. Отметим шапочкой регулярные обобщенные функции $\hat{u} = u(x,t), \quad \hat{G} = G(x,t)$.

Л е м м а 1.1. *Если u – классическое решение* (1), *то $\hat{u}$ является его обобщенным решением.*

Д о к а з а т е л ь с т в о. Если u имеет конечный разрыв на F, то в $S'(R^2)$, согласно правилам дифференцирования регулярных обобщенных функций ,

$$\hat{u}_{,j} = u_{,j} + [u]_F \nu_j \delta_F, \; x_1 = x, \; x_2 = \tau, \tag{4}$$

где первое слагаемое справа - классическая производная по x_j $(j = 1,2)$, $\nu = (\nu_x, \nu_\tau)$ - единичная нормаль к F , $\|\nu\| = 1$, δ_F - простой слой на F - сингулярная обобщенная функция, которая определяет функционал в виде поверхностного интеграла:

$$([u]_F \nu_j \delta_F(x,\tau), \phi(x,\tau)) = \int_F [u(x,\tau)]_F \nu_j(x,\tau)\phi(x,\tau) dF(x,\tau)$$

для $\forall \phi \in S(R^2)$. Поэтому, с учетом (4) и условий Адамара (3), получим

$$\hat{u}_{,j} = u_{,j} + [u]_F \nu_j \delta_F(x,\tau) = u_{,j}\,, \tag{5}$$

$$\hat{u}_{,jj} = u_{,jj} + [u_{,j}]_{F_t} \nu_j \delta_F(x,\tau), \quad j = 1,2. \tag{6}$$

Поскольку $\hat{u}_{,\tau} = c^{-1} u_{,t}\,, \quad \hat{u}_{,\tau\tau} = c^{-2} u_{,tt} - c^{-1} [u_{,t}]_{F_t} \nu_\tau \delta_F$. с учетом этих равенств и условий Адамара (3), получим

$$\Box \hat{u} = u_{,xx} - u_{,\tau\tau} + \left\{\nu_x [u_{,x}]_F - \nu_\tau [u_{,\tau}]_F\right\} \delta_F =$$

$$= G + \nu_x \left([u_{,x}]_{F_t} + [u_{,\tau}]_{F_t}\right) \delta_F = G,$$

так как плотности слоев равны нулю. Что и требовалось доказать.

Замечание 1. Из этой леммы следует, что условия на фронтах ударных волн легко получить, рассматривая классические решения гиперболических уравнений как обобщенные. Достаточно приравнять нулю плотности соответствующих независимых сингулярных обобщенных функций – аналогов простых, двойных и др. слоев, возникающих при обобщенном дифференцировании решений. Определение таких условий на основе классических методов весьма трудоемкая процедура.

2. Постановка начально-краевых задач

Требуется найти решение волнового уравнения $u(x,t)$ при $t \geq 0$ в области $S^- = \{x : x \in (0,L)\}$, удовлетворяющее следующим начальным и граничным условиям при $x \in S = \{x = 0, \; x = L\}$.

Начальные условия Коши. При $t = 0$

$$u(x,0) = u_0(x) \text{ для } x \in S^- + S, \quad u_{,t}(x,0) = v_0(x) \quad \text{для } x \in S^-. \tag{7}$$

Здесь вначале рассмотрим три краевые задачи с локальными граничными условиями, соответствующими условиям Дирихле и Неймана на концах стержня.

Граничные условия:

(КЗ I)

$$u(x,t) = w_j(t) \text{ для } x \in S, \; t \geq 0; \tag{8}$$

(КЗ II)

$$\frac{\partial u}{\partial x} = p_j(x,t) \quad \text{для } x \in S, \; t \geq 0; \tag{9}$$

(КЗ III)

$$u(0,t)=w(t),\quad \frac{\partial u}{\partial x}=p(L,t)\quad \text{для } t\geq 0. \tag{10}$$

Здесь j=1,2 соответственно левому и правому краю отрезка $[0,L]$.

Для первой краевой задачи выполнены условия согласования граничных и начальных данных:

$$u_0(x)=w_j,\quad j=1,2,\quad \text{для}\, x\in S. \tag{11}$$

На волновых фронтах, если они возникают, выполняются условия Адамара (3). Заметим, что ударные волны всегда возникают, если не выполнено условие согласования начальных и граничных данных по скоростям для $x\in S$:

$$\dot{u}(x,0)=v_0(x)\quad \text{для}\, x=0,\ x=L, \tag{12}$$

что типично для физических задач (здесь и далее $\partial_t u=\dot{u}$). В этом случае в начальный момент времени на границе S формируется фронт ударной волны, который распространяется со скоростью c в S^- . Для построения непрерывно дифференцируемых решений условие (12) является необходимым.

Предполагается, что начальные условия заданы и известно одно из граничных условий соответственно рассматриваемой краевой задаче. Единственность решения поставленных начально-краевых задач с учетом ударных волн для уравнения Даламбера в пространствах размерности 1,2,3 показана в [12,13].

3. Постановка начально-краевой задачи в $S'(R^2)$ и ее обобщенное решение

Для построения решения КЗ перейдем в пространство обобщенных функций медленного роста $S'(R^2)$ [14,15]. Для этого введем характеристическую функцию области определения решения

$$H_D^-(x,t)\equiv H_S^-(x)\,H(t),$$

где $H_S^-(x)=H(x)H(L-x)$ - характеристическая функция множества S^-, равная 0,5 на его границе S, $H(t)$ - функция Хевисайда, равная 0,5 при t=0.

Введем регулярные обобщенные функции, доопределенные нулем вне области решения КЗ:

$$\hat{u}(x,t)=u(x,t)H_D^-(x,t),\ \hat{G}(x,t)=G(x,t)H_S^-(x)\,H(t),$$

где $u(x,t)$ - классическое решение КЗ. Легко показать, что их обобщенные частные производные равны:

$$\hat{u}_{,x}=u_{,x}\,H_D^-+u(0,t)\delta(x)H(t)-u(L,t)\delta(x-L)H(t),$$

$$\hat{u}_{,xx}=u_{,xx}\,H_D^-+u_{,x}\,(0,t)\delta(x)H(t)-u_{,x}\,(L,t)\delta(x-L)H(t)+$$

$$+u(0,t)\delta'(x)H(t)-u(L,t)\delta'(x-L)H(t), \tag{13}$$

$$\hat{u}_{,t}=u_{,t}\,H_D^-+u(x,0)\delta(t),$$

$$\hat{u}_{,tt}=u_{,tt}\,H_D^-+u_{,t}\,(x,0)\delta(t)H(x)H(L-x)+u(x,0)\delta'(t).$$

где $\delta(...)$ - сингулярная дельта-функция (функция Дирака). Если решение имеет скачки на волновых фронтах, то следует добавить соответствующие слагаемые из (5), (6). С учетом этих равенств и условий Адамара на фронтах, получим уравнение в $S'(R^2)$:

$$\Box_c\hat{u}=\hat{G}+u_{,x}\,(0,t)\delta(x)H(t)-u_{,x}\,(L,t)\delta(x-L)H(t)+$$

$$+u(0,t)\delta'(x)H(t)-u(L,t)\delta'(x-L)H(t)- \tag{14}$$

$$-c^{-2}\left\{u_{,t}\,(x,0)\delta(t)+u(x,0)\delta'(t)\right\}H(x)H(L-x)$$

Решением этого уравнения является свертка фундаментального решения уравнения с его правой частью. В качестве такого возьмем фундаментальное решение $\hat{U}(x,t)$:

$$\Box_c U = \delta(x)\delta(t), \tag{15}$$

удовлетворяющее условиям излучения:

$$\hat{U}(x,t) = 0 \text{ при } t < 0, \quad \hat{U}(x,t) = 0 \text{ при } \|x\| > ct.$$

Решением его является функция Римана[14,15] :

$$\hat{U}(x,t) = -\frac{c}{2} H(ct - |x|). \tag{16}$$

Эта свертка дает обобщенное решение краевых задач:

$$\begin{gathered}
\hat{u} = \hat{G} * \hat{U} + u_{,x}(0,t)\delta(x)H(t) * \hat{U} - u_{,x}(L,t)\delta(x-L)H(t) * \hat{U} + \\
+ u(0,t)\delta'(x)H(t) * \hat{U} - u(L,t)\delta'(x-L)H(t) * \hat{U} - \\
- c^{-2}\left\{u_{,t}(x,0)\delta(t)H(x)H(L-x) * \hat{U} + u(x,0)\delta'(t) * \hat{U}\right\} = \\
= \hat{G} * \hat{U} + p_1(t)H(t) \underset{t}{*} \hat{U}(x,t) - p_2(t)H(t) \underset{t}{*} \hat{U}(x-l,t) + \\
+ w_1(t)H(t) \underset{t}{*} \partial_x \hat{U}(x,t) - w_2(t)H(t) \underset{t}{*} \partial_x \hat{U}(x-l,t) + \\
- c^{-2}\left\{v_0(x)H(x)H(L-x) \underset{x}{*} \hat{U}(x) + u_0(x)H(x)H(L-x) \underset{x}{*} \partial_t \hat{U}\right\}
\end{gathered} \tag{17}$$

Его интегральное представление дает следующая теорема.

Т е о р е м а 1. *Решение начально краевых задач для уравнения Даламбера на отрезке* (a_1, a_2) *имеет вид*:

$$\begin{gathered}
2\hat{u} = c\left\{H(ct - |x-a_2|)\int_{\frac{|x-a_2|}{c}}^{t} u_{,x}(a_2,\tau)\,d\tau - H(ct-|x-a_1|)\int_{\frac{|x-a_1|}{c}}^{t} u_{,x}(a_1,\tau)\,d\tau\right\} + \\
+ \operatorname{sgn}(x-a_1) H(ct-|x-a_1|)\, u\left(a_1, t - \frac{|x-a_1|}{c}\right) - \\
- \operatorname{sgn}(x-a_2) H(ct-|x-a_2|)\, u\left(a_2, t - \frac{|x-a_2|}{c}\right) + \\
+ c^{-1}\int_{a_1}^{a_2} \dot{u}_0(y)\, H(ct-|x-y|)dy + u_0(x+ct)\, H_S^-(x+ct) + \\
+ u_0(x-ct)\, H_S^-(x-ct) + 2\hat{G} * \hat{U}.
\end{gathered}$$

Здесь $a_1 = 0,\ a_2 = L$.

По аналогии с представлением решений уравнения Лапласа, эту формулу можно назвать *динамическим аналогом формулы Грина.* Она позволяет по граничным значениям функции и ее производных определять решние во всей области определения.

Для $x \in S$ формула дает 2 граничных интегральных уравнения для определения двух неизвестных граничных функций соответственно решаемой краевой задаче. В частности, при нулевых начальных условиях и правой части разрешающие граничные уравнения имеют вид:

$$\begin{gathered}
u(0,t) = c\left\{H(ct-L)\int_0^t u_{,x}(L,\tau)\,d\tau - H(t)\int_0^t u_{,x}(0,\tau)\,d\tau\right\} + \\
+ H(ct-L)\, u\left(L, t - \frac{L}{c}\right),
\end{gathered}$$

$$u(L,t)=c\left\{H\left(t\right)\int_0^t u_{,x}\left(L,\tau\right)d\tau-H\left(ct-L\right)\int_{\frac{L}{c}}^t u_{,x}\left(0,\tau\right)d\tau\right\}+$$

$$+H\left(ct-L\right)u\left(0,t-\frac{L}{c}\right).$$

Доказательство этих граничных уравнений следует из предельного перехода в формуле теоремы 1 к граничным точкам области [12].

4. Трансформанты Фурье решений краевых задач по времени

Для построения решения граничных уравнений удобно использовать прямое и обратное преобразования Фурье по времени, которые имеют вид:

$$\widehat{u}\ (x,\omega)=\int_{-\infty}^{\infty}u(x,t)e^{i\omega t}dt,\quad u(x,t)=\frac{1}{2\pi}\int_{-\infty}^{\infty}\widehat{u}\ (x,\omega)e^{-i\omega t}d\omega \tag{18}$$

Используя свойства преобразования Фурье сверток и производных [14,15], получим из (17) трансформанту Фурье обобщенного решения:

$$\begin{gathered}\widehat{u}\ (x,\omega)H(x)H(L-x)=\widehat{G}\underset{x}{*}\widehat{U}+\widehat{p}_1\ (\omega)\ \widehat{U}\ (x,\omega)-\widehat{p}_2\ (\omega)\ \widehat{U}\ (x-L,\omega)+\\ +\widehat{w}_1\ (\omega)\partial_x\ \widehat{U}\ (x,\omega)-\widehat{w}_2\ (\omega)\partial_x\ \widehat{U}\ (x-L,\omega)+\\ -^{-2}\left\{v_0(x)H(x)H(L-x)\underset{x}{*}\widehat{U}-i\omega u_0(x)\underset{x}{*}\widehat{U}\right\}\end{gathered} \tag{19}$$

Здесь ω - переменная Фурье по времени, $\widehat{U}\ (x,\omega)$ - преобразование Фурье по времени функции Римана:

$$\begin{gathered}\widehat{U}_{,xx}+k^2\ \widehat{U}=\delta(x),\quad k=\tfrac{\omega+i0}{c},\\ \widehat{U}\ (x,\omega)=0,5k^{-1}\sin(k\left|x\right|),\quad \widehat{U}_{,x}=0,5\cos(k\left|x\right|)\mathrm{sgn}(x),\\ \mathrm{sgn}\,x=\begin{cases}1, & x>0\\ 0, & x=0\\ -1, & x<0\end{cases}\end{gathered} \tag{20}$$

В результате получим трансформанту решения:

$$\begin{gathered}\widehat{u}\ (x,\omega)H(x)H(L-x)=\widehat{G}\underset{x}{*}\widehat{U}+0,5k^{-1}\ \widehat{p}_1\ (\omega)\sin(k\left|x\right|)-\\ -0,5k^{-1}\ \widehat{p}_2\ (\omega)\sin(k\left|x-L\right|)+\\ +0,5\ \widehat{w}_1\ (\omega)\cos(k\left|x\right|)-0,5\ \widehat{w}_2\ (\omega)\cos(k\left|x-L\right|)+\\ -0,5k^{-1}c^{-2}\left\{v_0(x)H(x)H(L-x)\underset{x}{*}\sin(k\left|x\right|)-i\omega u_0(x)\underset{x}{*}\sin(k\left|x\right|)\right\}\end{gathered} \tag{21}$$

Если перейти в этой формуле к пределу к левому и правому краю интервала, с учетом свойства производной $U_{,x}$ (20), получим линейные алгебраические уравнения для определения неизвестных граничных функций:

$$\begin{gathered}0.5\ \widehat{w}_1\ (\omega)=\widehat{G}\underset{x}{*}\widehat{U}\Big|_{x=0}-0,5k^{-1}\ \widehat{p}_2\ (\omega)\sin(kL)-0,5\ \widehat{w}_2\ (\omega)\cos(kL)+\\ -0,5c^{-2}k^{-1}\ (v_0(x)-i\omega u_0(x))\ H(x)H(L-x)\underset{x}{*}\sin(k\left|x\right|)\Big|_{x=0}\end{gathered}$$

$$0.5\ \widehat{w}_2\ (\omega) = \widehat{G} \underset{x}{*} \widehat{U}\Big|_{x=L} + 0,5k^{-1}\ \widehat{p}_1\ (\omega)\sin(kL) + 0,5\ \widehat{w}_1\ (\omega)\cos(kL) +$$

$$-0,5c^{-2}k^{-1}\ (v_0(x) - i\omega u_0(x))\, H(x)H(L-x) \underset{x}{*} \sin(k\,|x|)\Big|_{x=L}$$

Эту систему перепишем в матричном виде:

$$\left\{ \begin{array}{cc} 1, & 0 \\ -\cos kL, & -k^{-1}\sin kL \end{array} \right\} \left\{ \begin{array}{c} \widehat{w}_1\ (\omega) \\ \widehat{p}_1\ (\omega) \end{array} \right\} +$$

$$+ \left\{ \begin{array}{cc} \cos kL, & k^{-1}\sin kL \\ 1, & 0 \end{array} \right\} \left\{ \begin{array}{c} \widehat{w}_2\ (\omega) \\ \widehat{p}_2\ (\omega) \end{array} \right\} = \left\{ \begin{array}{c} F_1(\omega) \\ F_2(\omega) \end{array} \right\}, \tag{22}$$

где правые части известны:

$$F_1(\omega) = \widehat{G} \underset{x}{*} \widehat{U}\Big|_{x=0} - 0,5c^{-2}k^{-1}\ (v_0(x) - i\omega u_0(x))\, H(x)H(L-x) \underset{x}{*} \sin(k\,|x|)\Big|_{x=0}$$

$$F_2(\omega) = \widehat{G} \underset{x}{*} \widehat{U}\Big|_{x=L} - 0,5c^{-2}k^{-1}\ (v_0(x) - i\omega u_0(x))\, H(x)H(L-x) \underset{x}{*} \sin(k\,|x|)\Big|_{x=L}$$

Здесь значение свертки в правой части берется в указанной точке на левом или правом концах отрезка.

В зависимости от решаемой краевой задачи из этой системы получим разрешающие уравнения для определения неизвестных граничных функций.

Первая краевая задача

$$\begin{array}{l} \widehat{p}_1\ (\omega) = -\frac{2F_2 - \cos(kL)\widehat{w}_1(\omega) - \widehat{w}_2(\omega)}{k^{-1}\sin(kL)} \\ \widehat{p}_2\ (\omega) = -\frac{2F_1 - \cos(kL)\widehat{w}_2(\omega) - \widehat{w}_1(\omega)}{k^{-1}\sin(kL)} \end{array} \tag{23}$$

Вторая краевая задача

$$\left\{ \begin{array}{cc} 1, & \cos(kL) \\ -\cos(kL), & 1 \end{array} \right\} \left\{ \begin{array}{c} \widehat{w}_1\ (\omega) \\ \widehat{w}_2\ (\omega) \end{array} \right\} = \left\{ \begin{array}{c} 2F_1 - k^{-1}\sin(kL)\ \widehat{p}_2\ (\omega) \\ 2F_2 + k^{-1}\sin(kL)\ \widehat{p}_1\ (\omega) \end{array} \right\} = \left\{ \begin{array}{c} f_1(\omega) \\ f_2(\omega) \end{array} \right\}$$

$$\widehat{w}_j\ (\omega) = \frac{\Delta_j(\omega)}{\Delta(\omega)}, \quad \Delta(\omega) = 1 + \cos^2(kL), \tag{24}$$

$$\Delta_1 = f_1(\omega) - f_2(\omega)\cos(kL(, \quad \Delta_2 = f_2(\omega) + f_1(\omega)\cos(kL).$$

Третья краевая задача

$$\begin{array}{l} \widehat{w}_2\ (\omega) = \frac{2F_1(\omega) - \widehat{w}_1(\omega) - k^{-1}\sin(kL)\widehat{p}_2(\omega)}{\cos(kL)}, \\ \widehat{p}_1\ (\omega) = -\frac{2F_2(\omega) + \cos(kL)\widehat{w}_1(\omega) - 2\widehat{w}_2(\omega)}{k^{-1}\sin(kL)}. \end{array} \tag{25}$$

Выполняя обратное преобразование (18), получим оригинал решения в исходном пространстве-времени.

5. Разрешающие уравнения краевых задач с локальными и нелокальными краевыми условиями

Система из двух уравнений (22) связывает 4 граничные функции, из которых 2 неизвестны. Поэтому она позволяет ставить различные краевые задачи, кроме вначале представленных.

Для решения всех поставленных краевых задач удобно рассмотреть расширенную систему уравнений вида:

$$\left\{\begin{array}{cccc} 0,5 & 0 & 0,5\cos(kL) & 0,5k^{-1}\sin(kL) \\ -0,5\cos(kL) & -0,5k^{-1}\sin(kL) & 0,5 & 0 \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right\} \times$$

$$\times \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \\ \widehat{w}_2(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\} = \left\{\begin{array}{c} F_1(\omega) \\ F_2(\omega) \\ \widehat{b}_1(\omega) \\ \widehat{b}_2(\omega) \end{array}\right\}, \tag{26}$$

где последние два уравнения – это краевые условия:

$$\left\{\begin{array}{cc} a_{31} & a_{32} \\ a_{41} & a_{42} \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \end{array}\right\} + \left\{\begin{array}{cc} a_{33} & a_{34} \\ a_{43} & a_{44} \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_2(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\} = \left\{\begin{array}{c} \widehat{b}_1(\omega) \\ \widehat{b}_2(\omega) \end{array}\right\}, \tag{27}$$

которые связывают граничные значения решения и его производных на концах отрезка. При заданных коэффициентах a_{ij} и правой части $\widehat{b}_i(\omega)$ этой линейной алгебраической системы уравнений ее решение имеет вид:

$$D_j(\omega) = \frac{\Delta_j(\omega)}{\Delta(\omega)}, \quad D(\omega) = \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \\ \widehat{w}_2(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\}, \tag{28}$$

где $\Delta(\omega)$ - определитель матрицы системы (22), $\Delta_j(\omega)$ определитель матрицы, которая определяется простым правилом Крамера для каждого $D_j(\omega)$. В частности, для представленных решений краевых задач компоненты расширенной матрицы будут иметь следующий вид:

(КЗ I)

$$\left\{\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \end{array}\right\} + \left\{\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_2(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\} = \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{w}_2(\omega) \end{array}\right\};$$

(КЗ II)

$$\left\{\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \end{array}\right\} + \left\{\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_2(\omega) \\ \widehat{p}_1(\omega) \end{array}\right\} = \left\{\begin{array}{c} p_1(\omega) \\ p_2(\omega) \end{array}\right\};$$

(КЗ III)

$$\left\{\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_1(\omega) \end{array}\right\} + \left\{\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}\right\} \left\{\begin{array}{c} \widehat{w}_2(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\} = \left\{\begin{array}{c} \widehat{w}_1(\omega) \\ \widehat{p}_2(\omega) \end{array}\right\}.$$

Очевидно, что задавая различные коэффициенты и правые части уравнений, разработанный метод позволяет решать задачи с краевыми условиями самого различного вида, как с локальными условиями на одном и другом концах стержня, так и не локальными, связывающими краевые условия на его концах. Поскольку для четырех граничных функций имеем два граничных уравнения, то можно задавать еще два линейных уравнения на граничные значения функции и ее производной.

Вопрос разрешимости краевых задач будет определяться разрешимостью расширенной системы уравнений (23). Нули определителя этой системы ω_k:

$$\Delta(\omega_k) = 0, \tag{29}$$

определяют спектр свободных колебаний, который зависит от рассматриваемых краевых условий.

6. Построение оригиналов решений нестационарных краевых задач

Подставляя преобразование Фурье граничных функций в формулу (23) и выполняя обратное преобразование Фурье решения краевой задачи, получим оригинал решения в исходном пространстве-времени.

Вычислим вначале в формуле слагаемые, связанное с известными правой частью и начальными условиями, которые для регулярных функций имеют интегральное представление:

$$\begin{gathered}\hat{G} * \hat{U} = H(t) \int_0^t d\tau \int_0^x G(y,\tau) U(x-y, t-\tau) dy = \\ = H(t) \int_0^t d\tau \int_0^x G(y, t-\tau) H(c\tau - |x-y|) dy = u1(x,t)\end{gathered} \tag{30}$$

$$\begin{gathered}-u2(x,t) = \tfrac{1}{2c}\{v_0(x)H(x)H(L-x) \underset{x}{*} H\left(ct-|x|\right) + \\ + \tfrac{1}{2c} u_0(x)H(x)H(L-x) \underset{x}{*} \delta\left(ct-|x|\right)\operatorname{sgn}(x)\} = \\ = \tfrac{1}{2c}\{H(t)\textstyle\int_0^L v_0(y) H\left(ct-|x-y|\right) dy + \\ + u_0(x-ct)H_S^-(x-ct) - u_0(x+ct)H_S^-(x+ct)\}\end{gathered} \tag{31}$$

Заметим, что если $\hat{G}$ является сингулярной обобщенной функцией, то свертку в формуле нужно брать согласно определению свертки в пространстве обобщенных функций.

Теперь рассмотрим оставшиеся слагаемые, обусловленные краевыми условиями, которое формально можно записать в виде:

$$u3(x,t) = \tfrac{H(t)}{2\pi} \textstyle\int_{-\infty}^{\infty} e^{i\omega t} \left\{ p_1(\omega)\, \widehat{U}\,(x,\omega) - \widehat{p}_2\,(\omega)\, \widehat{U}\,(x-L,\omega) \right\} d\omega$$

$$u4(x,t) = -\tfrac{H(t)}{2\pi} \textstyle\int_{-\infty}^{\infty} \omega\, e^{i\omega t} \left\{ \widehat{w}_1\,(\omega)\, \widehat{U}\,(x,\omega) - \widehat{w}_2\,(\omega)\, \widehat{U}\,(x-L,\omega) \right\} d\omega$$

Поскольку носитель по t положительная полуось, то

$$u3(x,t) = \tfrac{c}{4\pi} \textstyle\int_{-\infty}^{\infty} \left\{ p_1(\omega) \sin\frac{\omega x}{c} - \widehat{p}_2\,(\omega) \sin\frac{\omega(L-x)}{c} \right\} \frac{e^{i\omega t}}{\omega + i0} d\omega$$

$$u4(x,t) = -\tfrac{c}{4\pi} \textstyle\int_{-\infty}^{\infty} \left\{ \widehat{w}_1\,(\omega) \sin\frac{\omega x}{c} - \widehat{w}_2\,(\omega) \sin\frac{\omega(L-x)}{c} \right\} e^{i\omega t} d\omega$$

Вычисление этих интегралов зависит от вида решаемой краевой задачи .

6.1. **Представление решения краевой задачи I.** Рассмотрим

$$\begin{gathered}u3(x,t) = \tfrac{c}{4\pi} \textstyle\int_{-\infty}^{\infty} \left\{ \widehat{p}_1\,(\omega) \sin\frac{\omega x}{c} - \widehat{p}_2\,(\omega) \sin\frac{\omega(L-x)}{c} \right\} \frac{e^{i\omega t}}{\omega + i0} d\omega \triangleq \\ = \tfrac{c}{4\pi} \lim_{\varepsilon \to +0} \textstyle\int_{-\infty}^{\infty} \left\{ \widehat{p}_1\,(\omega) \sin\frac{\omega x}{c} - \widehat{p}_2\,(\omega) \sin\frac{\omega(L-x)}{c} \right\} \frac{e^{i\omega t}}{\omega + i\varepsilon} d\omega,\end{gathered}$$

$t \geq 0$, $x \in [0, L]$. Обозначим

$$u31(x,t) = \frac{c}{4\pi} \lim_{\varepsilon \to +0} \int_{-\infty}^{\infty} \left\{ \widehat{p}_1(\omega) \sin \frac{\omega x}{c} \right\} \frac{e^{i\omega t}}{\omega + i\varepsilon} d\omega,$$

$$u32(x,t) = \frac{c}{4\pi} \lim_{\varepsilon \to +0} \int_{-\infty}^{\infty} \left\{ \widehat{p}_2(\omega) \sin \frac{\omega(x-L)}{c} \right\} \frac{e^{i\omega t}}{\omega + i\varepsilon} d\omega.$$

В случае первой краевой задачи подынтегральные функции не имеют особенность в нуле. Действительно, из формул (23) следует:

$$\widehat{p}_1(\omega) = -\frac{2F_2(\omega) - \widehat{w}_1(\omega)\cos(\omega L/c) - \widehat{w}_2(\omega)}{c \sin((\omega + i0)L/c)} \omega \Rightarrow$$

$$\widehat{p}_1(0) = -\frac{1}{L}\left(2F_2(0) - \widehat{w}_1(0) - \widehat{w}_2(0)\right);$$

$$\widehat{p}_2(\omega) = -\frac{2F_1 - \widehat{w}_2(\omega)\cos(\omega L/c) - \widehat{w}_1(\omega)}{c \sin((\omega + i0)L/c)} \omega \Rightarrow$$

$$\widehat{p}_2(0) = -\frac{1}{L}\left(2F_1(0) - \widehat{w}_2(0) - \widehat{w}_1(0)\right).$$

Вычислим $u3(x,t) = u31(x,t) + u32(x,t)$, переходя к пределу по $\varepsilon \to +0$ с обходом нулей знаменателя подынтегральной функции по ε-полуокружностям в комплексной верхней полуплоскости . В результате получим :

$$u31(x,t) =$$

$$= -\frac{1}{4\pi} V.P. \int_{-\infty}^{\infty} \left\{ 2F_2(\omega) - \widehat{w}_1(\omega)\cos(\omega L/) - \widehat{w}_2(\omega) \right\} \frac{\sin(\omega x/c)}{\sin((\omega + i0)L/c)} e^{i\omega t} d\omega +$$

$$+ \frac{1}{4} \sum_n \operatorname{Res} \left\{ \left\{ 2F_2(\omega) - \widehat{w}_1(\omega)\cos(\omega L/c) - \widehat{w}_2(\omega) \right\} \frac{\sin(\omega x/c)}{\sin((\omega + i0)L/c)} e^{i\omega t} \right\} |_{\omega = \omega_n} =$$

$$= -\frac{1}{4\pi} V.P. \int_{-\infty}^{\infty} \left\{ 2F_2(\omega) - \widehat{w}_1(\omega)\cos(\omega L/c) - \widehat{w}_2(\omega) \right\} \frac{\sin(\omega x/c)}{\sin((\omega + i0)L/c)} e^{i\omega t} d\omega +$$

$$+ \frac{1}{4} \sum_n (-1)^{n+1} \left\{ 2F_2(\omega_n) - \widehat{w}_1(\omega_n)\cos(\omega_n L/c) - \widehat{w}_2(\omega_n) \right\} \sin(\omega_n x/c) e^{i\omega_n t}.$$

Здесь точки $\omega_n = \pi n c/L$ $(n = \pm 1, \pm 2, ...)$, где знаменатель подынтегральной функции обращается в ноль. В окрестности этих точек интеграл следует брать в смысле главного значения. Здесь мы воспользовались леммой Жордана о вычетах при обходе полюсов функций, аналитических в их окрестности [16].

Аналогично получим

$$u32(x,t) = -\frac{c}{4\pi} \lim_{\varepsilon \to +0} \int_{-\infty}^{\infty} \left\{ \widehat{p}_2(\omega) \sin\left(c^{-1}\omega(L-x)\right) \right\} \frac{e^{i\omega t}}{\omega + i\varepsilon} d\omega =$$

$$= -\frac{1}{4\pi} V.P. \int_{-\infty}^{\infty} \left\{ 2F_1(\omega) - \widehat{w}_2(\omega)\cos(\omega L/c) - \widehat{w}_1(\omega) \right\} \frac{\sin(\omega(L-x)/c)}{\sin(\omega L/c)} e^{i\omega t} d\omega +$$

$$- \frac{1}{4} \sum_n (-1)^n \left\{ 2F_1(\omega_n) - \widehat{w}_1(\omega_n)\cos(\omega_n L/c) - \widehat{w}_2(\omega_n) \right\} \sin(\omega_n(L-x)/c) e^{i\omega_n t}.$$

Итак, оригиналы всех слагаемых в формуле (25) определены. Решение КЗ I построено.

Если известен вид заданных граничных функций, то формулы можно упростить. Как, например для упругой струны с неподвижными концами:

$$\widehat{w}_1 = \widehat{w}_2 = 0.$$

Следовательно,

$$u31(x,t) = \frac{1}{2} \sum_n (-1)^{n+1} \{F_2(\omega_n))\} \sin(\omega_n x/c) e^{i\omega_n t},$$

$$u32(x,t) = \frac{1}{2} \sum_n (-1)^{n+1} \{F_1(\omega_n))\} \sin(\omega_n(L-x)/c) e^{i\omega_n t}$$

Интегралы исчезли, поскольку интегралы с обходом полюсов по $\varepsilon-$ полуокружностям можно, по той же лемме, заменить суммой вычетов подынтегральной функции в ее полюсах.

Аналогично можно построить оригиналы всех поставленных краевых задач.

7. Заключение

Если действующие источники и граничные условия описываются периодическими по времени функциями, то разлагая их в ряды Фурье по времени, получим краевые задачи для каждой гармоники ряда, решение которых совпадает с построенным здесь решением в пространстве преобразований Фуцрье при нулевых начальных условиях.

Разработанный метод можно использовать для решения волновых уравнений на графах, используя построенные здесь разрешающие системы уравнений на каждом элементе графа и дополняя их условиями трансмиссии в узлах графа и на концах его элементов. Такая система зависит от строения графа. И она позволяет определять спектр резонансных частот для такого графа. С такими задачами авторы постараются познакомить читателя в следующей статье.

8. Благодарность

Работа выполнена при финансовой поддержке Комитета науки Министерства образования и науки республики Казахстан (грант AP09261033).

Список литературы

1 Покорный Ю.В., Пенкин О.М., Прядиев В.Л., Боровских А.В., Лазерев К.П., Шабров С.А. Дифференциальные уравнения на геометрических графах - Москва: ФИЗМАТЛИТ, 2004.

2 Покорный Ю.В., Прядиев В.Л., Боровских А.В. Волновое уравнение на пространственной сети // Докл. РАН. -2003. -Т. 38. № 1. -С. 16-18.

3 Kuchment P. Graph models of wave propagation in thin structures // Waves in Random Media. -2002. -Vol. 12. No 4. -P. 1-24.

4 Cattaneo C., Fontana L. D'Alambert formula on finite one-dimensional networks // Journal of Math. Anal. and Appl. -2003. -Vol. 28. No 2. -P. 403-424.

5 Pokorny Yu.V., Borovskikh A.V. Differential equations on networks (geometric graph) // Journal of Mathematical sciences. -2004. -Vol. 11. No 6. -P. 691-718.

6 Ильин В.А. Волновое уравнение с граничным управлением на одном конце при закрепленном втором конце // Диф. уравнения. -1999. -Т. 35. № 12. -С. 1640-1659.

7 Nicaise S., Valein J., Fridman E. Stability of the heat and wave equations with boundary time-varying delays // Discrete Contin. Dyn. Syst. -2009. -Vol. 12. No 2. -P. 559–581.

8 Valein J., Zuazua E. Stabilization of the wave equation on 1-D networks // SIAM J. Control Optim. -2009. -Vol. 48. No 4. -P. 2771–2797.

9 Боровских А.В., Копытин А.В. О распространении волн по сети // Сборник статей аспирантов и студентов математического факультета. - Воронеж, Воронеж. гос. ун-т., -1999. - С.21-25.

10 Копытин А.В., Прядиев В.Л. Об аналоге формулы Даламбера и спектре лапласиана на графе с соизмеримыми рёбрами // Вест. Воронежю гос. ун-та. Сер. Физика. Матаматика. - 2001. - № 1. -С. 104-107.

11 Копытин А.В., Прядиев В.Л. Решение волнового уравнения на пространственной сети // Сборник статей аспирантов и студентов математического факультета. - Воронеж, Воронеж. гос. ун-т. 2000. - С.19-23.

12 Алексеева Л.А. Метод обобщенных функций в нестационарных краевых задачах для волнового уравнения// Математический журнал. -2006. -Т. 6. № 1. -С. 16-32.

13 Alexeyeva L.A. Boundary integral equations of nonstationary BVP for wave equations// Int. Congress of Mathematicians, Abstracts, Madrid -2006. -P.436.

14 Владимиров В.С. Уравнения математической физики. - Москва: Наука, 1982.

15 Владимиров В.С. Обобщенные функции в математической физике. - Москва: Наука, 1978.

16 Лаврентьев М.А., Шабат Б.В.. Методы теории функций комплексного переменного. - Москва: Наука, 1976.

Л.А. Алексеева, Г.Д. Арепова

ҚР БжҒМ Математика және математикалық моделдеу институты, Пушкин 125, Алматы, Қазақстан

Локалді және байланысты шекаралық шартты д'Аламбер теңдеуі үшін шекаралық есептердің жалпыланған шешімдері

Аннотация: Жалпы түрдегі сегменттің ұштарында локалді және локалді емес сызықтық шекаралық шарттары бар толқындық теңдеуі үшін бастапқы-шекаралық есептері қарастырылады. Оларды шешу үшін бастапқы шекаралық есептерді оң жағы тығыздығы ізделінді функция мен оның туындыларының шекаралық және бастапқы мәндері арқылы анықталатын қарапайым және қос қабатты сингулярлығы бар толқындық теңдеуді шешуге алып келетін жалпылама функциялар әдісі әзірленді. Толқындық теңдеудің шешімдері үшін Грин формуласының жалпылауы болып табылатын шекаралық функциялар арқылы өрнектелетін шешімнің интегралдық түрі алынды. Белгісіз шекаралық функцияларды анықтау үшін, уақыт бойынша Фурье түрлендіруі кеңістігінде 4 шекаралық шешімдері мен оның туындыларының мәндерін байланыстыратын екі сызықты алгебралық теңдеулерден тұратын шешуші жүйесі құрылды. Қойылған бастапқы-шекаралық есептерді шешу үшін локалді және локалді емес типтегі екі шекаралық шартпен бірге шешуші теңдеулер жүйесі құрылды. Оның негізінде кесіндінің ұштарында Дирихле, Нейман және аралас классикалық үш шекаралық есептердің аналитикалық шешімдері берілген. Әзірленген әдіс әртүрлі локалді және локалді емес шекаралық шартты шекаралық есептерді шешуге мүмкіндік береді және әртүрлі құрылымды графтардағы толқындық және басқа теңдеулерді шешуде қолданысы болуы керек.

Түйін сөздер: д'Аламбер теңдеуі, шекаралық есеп, бастапқы шарттар, шекаралық шарттар, жалпыланған функциялар әдісі, Риман функциясы, жалпылама шешім, шешуші теңдеулерді.

L.A. Alexeyeva, G.Zh. Arepova

Institute of Mathematics and Mathematical Modeling of MES RK, Pushkin str., 125, Almaty, Kazakhstan

Generalized Solutions of boundary value problems for the d'Alembert equation with local and associated boundary conditions

Abstract: The initial-boundary value problems for the wave equations with local and non-local linear boundary conditions at the ends of a general segment are considered. To solve them, a generalize functions method has been developed, which translates the original boundary value problems to solving the wave equation with a singular right-hand side containing a singular simple and double layers, the densities of which are determined by the boundary and initial values of the desired function and its derivatives. Received integral representation of the solution in terms of boundary functions, which are a generalization of Green's formula for solutions of the wave equation. To determine the unknown boundary functions, it is built in space Fourier transforms in time, a two-leaf resolving system linear algebraic equations, which connects 4 boundary values solution and its derivatives. Together with two boundary conditions of local and non-local type, a resolving system of equations is built for solving the stated initial-boundary value problems. On its basis, given analytical solutions for classical three boundary value problems with conditions Dirichlet, Neumann and mixed at the ends of the segment. The developed method allows solving boundary value problems with different local and nonlocal boundary conditions and must find an application change in solving wave and other equations on graphs of different structures.

Keywords: d'Alembert equation, boundary value problem, initial conditions, boundary conditions, generalized functions method, Riemann function, generalized solution, solving equations.

References

1 Pokorny Yu.V., Penkin O.M., Pryadiev V.L., Borovskikh A.V., Lazerev K.P., Shabrov S.A. Differencial'nye uravneniya na geometricheskih grafah [Differential Equations on Geometric Graphs] (FIZMATLIT, Moscow, 2004).

2 Pokorny Yu.V., Pryadiev V.L., Borovskikh A.V. Volnovoe uravnenie na prostranstvennoj seti [Wave equation on a spatial network], Dokl. RAN. 38(1), 16-18(2003).

3 Kuchment P. Graph models of wave propagation in thin structures, Waves in Random Media. 12(4), 1-24(2002).

4 Cattaneo C., Fontana L. D'Alambert formula on finite one-dimensional networks, Journal of Math. Anal. and Appl. 28(2), 403-424(2003).

5 Pokorny Yu.V., Borovskikh A.V. Differential equations on networks (geometric graph), Journal of Mathematical sciences, 11(6), 691-718(2004).

6 Ilyin V.A. Volnovoe uravnenie s granichnym upravleniem na odnom konce pri zakreplennom vtorom konce[Wave Equation with Boundary Control at One End with the Second End Fixed], Dif. equations, 35(12), 1640-1659(1999).

7 Nicaise S., Valein J., Fridman E. Stability of the heat and wave equations with boundary time-varying delays, Discrete Contin. Dyn. Syst., 12(2), 559–581(2009).

8 Valein J., Zuazua E. Stabilization of the wave equation on 1-D networks, SIAM J. Control Optim., 48(4), 2771–2797(2009).

9 Borovskikh A.V., Kopytin A.V. O rasprostranenii voln po seti [On the propagation of waves over the network], Sbornik statej aspirantov i studentov matematicheskogo fakul'teta [Collection of articles of graduate students and students of the Faculty of Mathematics]. Voronezh, Voronezh. state university, 1999. P.21-25.

10 Kopytin A.V., Pryadiev V.L. Ob analoge formuly Dalambera i spektre laplasiana na grafe s soizmerimymi ryobrami [On an analogue of the d'Alembert formula and the spectrum of the Laplacian on a graph with

commensurate edges], Vest. Voronezhyu gos. un-ta. Ser. Fizika. Matamatika [Vest. Voronezh state. university Ser. Physics. Mathematics]. 2001. No. 1. P. 104-107.
11 Kopytin A.V., Pryadiev V.L. Reshenie volnovogo uravneniya na prostranstvennoj seti [Solving the wave equation on a spatial network], Sbornik statej aspirantov i studentov matematicheskogo fakul'teta [Collection of articles of graduate students and students of the Faculty of Mathematics]. Voronezh, Voronezh. state university. 2000. P.19-23.
12 Alekseeva L.A. Metod obobshchennyh funkcij v nestacionarnyh kraevyh zadachah dlya volnovogo uravneniya [The method of generalized functions in non-stationary boundary value problems for the wave equation], Matematicheskij zhurnal [Mathematical journal]. 6(1), 16-32(2006).
13 Alexeyeva L.A. Boundary integral equations of nonstationary BVP for wave equations, Int. Congress of Mathematicians, Abstracts, Madrid, 2006. P.436.
14 Vladimirov V.S. Uravneniya matematicheskoj fiziki [Equations of mathematical physics]. (Nauka, Moscow, 1982).
15 Vladimirov V.S. [Generalized functions in mathematical physics]. (Nauka, Moscow, 1978).
16 Lavrentiev M.A., Shabat B.V. Metody teorii funkcij kompleksnogo peremennogo [Methods of the theory of functions of a complex variable]. (Nauka, Moscow, 1976).

Авторлар туралы мағлұмат:

Алексеева Людмила Алексеевна – ***автор для корреспонденции***, доктор физико-математических наук, професор, Институт математики и математического моделирования МОН РК, ул. Пушкина 125, Алматы, Казахстан.

Арепова Гаухар Джумабаевна – PhD, научный сотрудник, Институт математики и математического моделирования, Алма-Ата, Казахстан.

Alexeyeva Lyudmila A. – ***corresponding author***, Doctor of physical and mathematical sciences, professor, Institute of Mathematics and Mathematical Modeling of MES RK, 125 Pushkin Str., Almaty, Kazakhstan.

Arepova Gaukhar Zh. – PhD, Scientific researcher, Institute of Mathematics and Mathematical Modeling of MES RK, 125 Pushkin Str., Almaty, Kazakhstan.

Поступила в редакцию 01.02.2022

Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2022, Vol. 138, №1, P.36-44
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

IRSTI: **27.21**

A. Iosevich, S. Mkrtchyan and T. Shen

Department of Mathematics, University of Rochester, Rochester, NY
(E-mail: iosevich@math.rochester.edu)

Pinned point configurations and Hausdorff dimension [1]

Abstract: We prove that if the Hausdorff dimension of a compact subset E of $\mathbb{R}^d$ with $d \geq 2$ is sufficiently large, and if G is a star-like graph with two parts, and each of its parts is a rigid graph, then the Lebesgue measure in the appropriate dimension, of the set of distances in E specified by the graph is positive. We also prove that if $dim_{\mathcal{H}}(E)$ is sufficiently large, then

$$\int \nu_G(r\vec{t}) d\nu_G(\vec{t}) > 0,$$

where ν_G is the measure on the space of distances specified by G which is induced by a Frostman measure. In particular, this means that for any $r > 0$ there exist many configurations encoded by $\vec{t}$ with vertices in E such that the vertices of $r\vec{t}$ are also in E.

Keywords: finite point configurations, group actions, simplexes, Hausdorff dimension.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.3

2000 Mathematics Subject Classification: 28A75, 49Q15.

1. Introduction

Let G be a connected graph on $k+1$ vertices. Let $V = \{x^1, x^2, \ldots, x^{k+1}\}$ denote the vertex set and e_G the edge map, where $e_G(i,j) = 1$ if x^i and x^j are connected by an edge, and 0 otherwise. We will only consider undirected graphs with no self-edges, so $e_G(i,i) = 0$ and $e_G(i,j) = e_G(j,i)$ for all i, j. Let $\mathcal{E}(G)$ denote the edge set, namely

$$\big\{(i,j) \in V \times V : e(x^i, x^j) = 1\big\} / \sim,$$

where $\sim$ is the equivalence relation $(i,j) \sim (j,i)$.

Given such a graph and a compact subset of $\mathbb{R}^d$, we are interested in the set of various point-configurations specified by the graph. More precisely, given a Frostman measure on the compact set, we define the induced measure on the space of distances specified by the garph.

Definition 1. Let G be a graph as above, $E \subset \mathbb{R}^d$, $d \geq 2$ a compact set and μ a Frostman measure on E. Define the induced measure ν_G by the relation

$$\int f(\vec{t}) d\nu_G(\vec{t}) = \int \ldots \int f(D_G(x^1, \ldots, x^{k+1})) d\mu(x^1) d\mu(x^2) \ldots d\mu(x^{k+1}),$$

where $\vec{t} = \{t_{ij}\}_{(i,j) \in \mathcal{E}(G)}$ is a set of positive real numbers, $D_G(x^1, \ldots, x^{k+1})$ is a vector of length equal to $\#\mathcal{E}(G)$ with entries $|x^i - x^j|$ for $(i,j) \in \mathcal{E}(G)$, with the entries ordered in the dictionary order.

Given such a compact set and a graph, for point configurations in the set we define their distance-profiles specified by the graph.

[1]The first listed author is supported in part by the National Science Foundation grant no. HDR TRIPODS - 1934962. The work of the second listed author was partially supported by the Simons Foundation Collaboration Grant No. 422190.

Definition 2. Given a compact set $E \subset \mathbb{R}^d$, $d \geq 2$, define

$$\Delta_G(E) = \left\{ D_G(x^1, \dots, x^{k+1}) : x^j \in E \right\} \subset \mathbb{R}^{\#\mathcal{E}(G)}.$$

Also define

$$\Delta_G^r(E) = \left\{ \vec{t} \in \Delta_G(E) : r\vec{t} \in \Delta_G(E) \right\} \subset \Delta_G(E).$$

For $\epsilon > 0$, define a smooth approximation of ν_G on $\mathbb{R}^k$ by the density

$$\nu_G^\epsilon(\vec{t}) = \int \cdots \int \prod_{t_{ij} \in \mathcal{E}(G)} \sigma_{t_{ij}}^\epsilon(x^i - x^j)\, d\mu(x^1) ... d\mu(x^{k+1})$$

$$= \int \cdots \int \prod_{i=1}^n T_{G_i}^\epsilon(x^i)\, d\mu(x^1) ... d\mu(x^{k+1}),$$

where T_{G_i} encodes the part that belongs to G_i. Let $\sigma_{t_{ij}}$ be the normalized surface measure on the sphere of radius t_{ij} and $\sigma_{t_{ij}}^\epsilon(t) := \sigma_{t_{ij}} * \rho_\epsilon(t)$, with $\rho \in C_0^\infty(\mathbb{R}^d)$, $\rho \geq 0$, $supp(\rho) \subset \{|s| < 1\}$, $\int \rho = 1$, and $\rho_\epsilon(t) = \epsilon^{-d}\rho(\epsilon^{-1}t)$. Then each $\nu_G \in C_0^\infty$ and $\nu_G^\epsilon \to \nu_G$ weak* as $\epsilon \to 0$.

Thus,

$$\nu_G(\Delta_G^r(E)) = \lim_{\epsilon \to 0} \int_{\mathbb{R}^k} \nu_G^\epsilon(r\vec{t})\, d\nu_G(\vec{t}).$$

Definition 3. Let G be a graph that can be decomposed as follows. Let $G = \cup_i G_i$ where $G_1, \dots, G_n$ is a family of connected graphs. Suppose that any G_i has exactly one vertex in common with any other G_j if $i \neq j$, and no other vertices in common between G_i and G_j, and there are no edges connecting vertices in G_i to vertices in G_j if $i \neq j$ except for their common point. Then we call G *a star* of G_i.

In this paper, we consider the case when all such G_i are rigid. A graph being rigid essentially means that continuous motion of the points of the configuration maintaining the edge length constraints comes from a family of distance-preserving Euclidean motions. The precise definition is the following.

Definition 4. Given a graph G with $V = \{x^1, x^2, \dots, x^{k+1}\}$ being its vertex set, let K be the smallest graph containing G such that K is a complete graph. Let

$$F_G = \{|x^i - x^j|^2 : t_{ij} \text{ is an edge of } G\}.$$

An infinitesimal motion of G is $\vec{u} = (u^1, ..., u^{k+1})$, a $(k+1)$-tuple $\vec{u}$ of vectors $u^j \in \mathbb{R}^d$ such that $DF_G \cdot \vec{u} = 0$.

If the set of infinitesimal motion of G and the set of infinitesimal motion of K are the same set, then G is called an *infinitesimal rigid graph.*

For a detailed discussion of rigidity in this sense refer to [2].

Our main results are the following.

Theorem 1. *Let G be a star of 2 graphs $\{G_i\}$ such that both G_i are infinitesimally rigid. For every i let $k_i + 1$ be the number of vertices G_i has and set $k = k_1 + k_2$, so that G has $k+1$ vertices. If $k \geq 4$, $d \geq 2$ and E is a compact subset of $\mathbb{R}^d$ of Hausdorff dimension larger than $\frac{dk-d+1}{k}$ then*

$$\mathcal{L}^m(\Delta_G(E)) > 0, \tag{1}$$

where m is the number of edges of G.

Note, by the definition of a rigid graph, we have that if $k_1 > d$, to compute the number of its edges, each of the vertices has d components, and we subtract the dimension of the Euclidean motion group. So the number of edges of G_1 is $d(k_1+1) - \binom{d+1}{2}$. If $k_1 \leq d$, it has to be a k_1- simplex, so the number of edges of G_1 is $\binom{k_1+1}{2}$. Similarly for G_2, if $k_2 > d$, the number of edges of G_2 is $d(k_2+1) - \binom{d+1}{2}$ and if $k_2 \leq d$, the number of edges of G_2 is $\binom{k_2+1}{2}$.

Therefore, if $k_1, k_2 > d$,

$$m = \sum_{i=1}^{2} \left[d(k_i+1) - \binom{d+1}{2} \right] = d(k+1) - 2\binom{d+1}{2} = dk - d^2.$$

If $k_1 > d$ and $k_2 \leq d$,

$$m = d(k_1+1) - \binom{d+1}{2} + \binom{k_2+1}{2}.$$

If $k_1 \leq d$ and $k_2 > d$,

$$m = d(k_2+1) - \binom{d+1}{2} + \binom{k_1+1}{2}.$$

If $k_1, k_2 \leq d$,

$$m = \binom{k_1+1}{2} + \binom{k_2+1}{2}.$$

remark 1. Note, that the dimensional threshold we obtain is just the case $n = 2$. We expect that a similar result will be proved in the case for general n.

That said, the present result is still an improvement on currently available thresholds. Since the graph G in the above theorem is a subgraph of a $(k+1)-$ simplex, the results of [2] give that (1) holds when the Hausdorff dimension of E is larger than $d - \frac{1}{k+1}$. Since $d \geq 2$, our new bound $\frac{dk-d+1}{k}$ is an improvement. Also from [7], we know that (1) holds when the Hausdorff dimension is larger than $\frac{dk+1}{k+1}$. Since $\frac{dk+1}{k+1} > \frac{dk+1-d}{k}$ when $d \geq 2$, our threshold is an improvement on that as well.

In order to state our second result, we need the following definition.

Definition 5. Let $d \geq 2$, $k \geq 1$. Let G be a connected graph on $k+1$ vertices as above. Let E be a compact subset of $\mathbb{R}^d$, $d \geq 2$. Define

$$s_G = \inf \left\{ s : dim_{\mathcal{H}}(E) > s \Rightarrow \ \nu_G \text{ is absolutely continuous, and } \int \nu_G^2(\vec{t}) d\vec{t} < \infty \right\}.$$

We say s_G is the L^2 *-threshold* corresponding to the pair (G, E).

Allan Greenleaf, the first and second listed authors proved that if $G = K_{k+1}$, $k \leq d$, and $E \subset \mathbb{R}^d$, $d \geq 2$, is a compact set of Hausdorff dimension larger than s_G, then

$$\nu_G(\Delta_G^r(E)) > 0 \tag{2}$$

for any $r > 0$. Roughly speaking, this means that for any $r > 0$ there exists a statistically correct number of pairs of k-dimensional simplexes that are similar to one another with the similarity ratio equal to r. The purpose of the second main result is to establish this type of a result for star-like graphs.

Our second main result is the following.

Theorem 2. *Let E be a compact subset of $\mathbb{R}^d$. Let G be a star of 2 infinitesimally rigid graphs $\{G_i\}$. Suppose that*

$$\int \nu_{G_i}(r\vec{t}) d\nu_{G_i}(\vec{t}) > 0, \tag{3}$$

and $dim_{\mathcal{H}}(E) > s_{G_i}$ for all i. Then, if $dim_{\mathcal{H}}(E) > s = \max\{s_{G_i}\}$, we have

$$\int \nu_G(r\vec{t}) d\nu_G(\vec{t}) > 0. \tag{4}$$

2. Proof of Theorem 1

We first prove the following proposition, which will help us to prove Theorem 1.

Let $O_d(\mathbb{R})$ be the orthogonal group of rotations of $\mathbb{R}^d$ and given $\theta \in O_d(\mathbb{R})$ define the measure λ_θ on $\mathbb{R}^d$ via the relation

$$\int f(x)d\lambda_\theta(x) = \int\int f(u-\theta v)d\mu(u)d\mu(v).$$

Proposition. *Let G be a star of n graphs $\{G_i\}$ such that all G_i are infinitesimally rigid. For every i let k_i+1 be the number of vertices G_i has and set $k=\prod_{i=1}^n k_i$, so that G has $k+1$ vertices. Then*

$$\int \nu_G^2(\vec{t})d\vec{t} < \infty$$

if and only if

$$\lim_{\epsilon\to 0^+}\int\cdots\int \lambda_{\theta_1}^\epsilon(x-\theta_1 x')^{k-n+1}\prod_{i=2}^n \lambda_{\theta_i}^\epsilon(x-\theta_i x')d\mu(x)d\mu(x')\prod_{i=1}^n d\theta_i < \infty,$$

where λ^ϵ denotes the convolution of λ with the approximation to the identity at level ϵ.

P r o o f. Let ν_G^ϵ denote the convolution of ν_G with the approximation to the identity at level ϵ. We'll prove the proposition by induction on the number of components n of the star graph G. First, suppose that $n=2$.

Using the same method as in Proposition 3.1 in [6], we can directly get

$$\liminf_{\epsilon\to 0}\int \nu_G^\epsilon(\vec{t})d\nu_G(\vec{t}) \approx \int\cdots\int \lambda_\theta^\epsilon(x-\theta x')^{k_1}\lambda_\phi^\epsilon(x-\phi x')^{k_2}d\mu(x)d\mu(x')d\theta d\phi \tag{5}$$

where x is the common vertex of G_1 and G_2, θ and ϕ correspond to the rotation of G_1 and G_2 respectively.

Here and thereafter, $X \lesssim Y$ means there exists a constant C such that $X \le CY$. The relation $X \gtrsim Y$ is defined similarly. In addition we write $X \approx Y$ if both $X \lesssim$ and $X \gtrsim Y$ hold.

Then by the Three Line Lemma, the right-hand side of (5) can be approximated as

$$\approx \int\cdots\int \lambda_\theta^\epsilon(x-\theta x')^{k-1}\lambda_\phi^\epsilon(x-\phi x')d\mu(x)d\mu(x')d\theta d\phi,$$

which corresponds to an infinitesimal rigid graph with k vertices with an extra edge added.

Therefore,

$$\liminf_{\epsilon\to 0}\int {\nu_G^\epsilon}^2(\vec{t})d\vec{t} < \infty$$

if and only if

$$\int\cdots\int \lambda_\theta^\epsilon(x-\theta x')^{k-1}\lambda_\phi^\epsilon(x-\phi x')d\mu(x)d\mu(x')d\theta d\phi < \infty.$$

For general n, using the same method when we are dealing with n=2, we can directly get

$$\liminf_{\epsilon\to 0}\int \nu_G^\epsilon(\vec{t})d\vec{t} \approx \int\cdots\int \lambda_{\theta_1}^\epsilon(x-\theta_1 x')^{k_1}\nu_{G'}^\epsilon(\vec{t'})d\mu(x)d\mu(x')d\theta_1 d\vec{t'} \tag{6}$$

where G' is the subgraph of G containing only $G_2,...,G_n$, and $\vec{t'}$ correspond to $\mathcal{E}(G')$, which is the edge set of G', and x is the common vertex of all G_i.

By the inductive hypothesis, (6) is

$$\approx \int\cdots\int \lambda_{\theta_1}^\epsilon(x-\theta_1 x')^{k_1}\lambda_{\theta_2}^\epsilon(x-\theta_2 x')^{\sum_{i=2}^{n-1}k_i-n+2}\lambda_{\theta_n}^\epsilon(x-\theta_n x')d\mu(x)d\mu(x')d\theta_1 d\theta_2 d\theta_n,$$

and applying the case $n = 2$, we get this is

$$\approx \int \cdots \int \lambda^{\epsilon}_{\theta_1}(x - \theta_1 x')^{k-n+1} \prod_{i=2}^{n} \lambda^{\epsilon}_{\theta_i}(x - \theta_i x') d\mu(x) d\mu(x') \prod_{i=1}^{n} d\theta_i,$$

finishing the proof of Proposition 2.

We're now ready to prove Theorem 1:

P r o o f. [Proof of Theorem 1]

By Proposition 2, we only need to estimate

$$\int \cdots \int \lambda^{\epsilon}_{\theta_1}(x - \theta_1 x')^{k-1} \lambda^{\epsilon}_{\theta_2}(x - \theta_2 x') d\mu(x) d\mu(x') d\theta_1 d\theta_2. \tag{7}$$

Since (7) corresponds to a graph which is a star of graphs with all except one of its components being a single edge, let's use t to denote the edge corresponding to λ_{θ_2} in this new graph. Then (7) is equal to

$$\int \cdots \int \lambda^{\epsilon}_{\theta_1}(x - \theta_1 x')^{k-1} \left(\sigma^{\epsilon}_t * \mu(x) \sigma^{\epsilon}_t * \mu(x')\right) d\mu(x) d\mu(x') d\theta_1 dt \tag{8}$$

Let κ_θ be defined similarly to λ_θ, via the relation

$$\int f(x) d\kappa_{\theta,t}(x) = \int \int f(u - \theta v) \cdot \sigma^{\epsilon}_t * \mu(u) \sigma^{\epsilon}_t * \mu(v) d\mu(u) d\mu(v).$$

Then by this definition, we get that (8) is equal to

$$\int \cdots \int \lambda^{\epsilon}_{\theta_1}(z)^{k-1} \kappa^{\epsilon}_{\theta_1,t}(z) dz d\theta_1 dt.$$

We use the Littlewood-Paley decomposition of it, and here the Littlewood-Paley piece is defined by $\hat{\lambda}_{\theta,j} = \hat{\lambda}_\theta(\xi)\rho(2^{-j}\xi)$, where ρ is a nonnegative bump function supported on $\{\frac{1}{2} \leq ||\xi|| \leq 2\}$, such that $\sum_j \rho_j(\xi) = 1$ for all ξ where $\rho_j(\xi) = \rho(2^{-j}\xi)$.

So we have that (7) is

$$= \sum_{j_0, j_1, \ldots, j_{k-1}} \int \cdots \int \lambda^{\epsilon}_{\theta_1, j_1}(z) \ldots \lambda^{\epsilon}_{\theta_1, j_{k-1}}(z) \kappa^{\epsilon}_{\theta_1, t, j_0}(z) dz d\theta_1 dt$$

$$\approx \sum_{j_0} \sum_{0 \leq j_1 \leq \cdots \leq j_{k-1}} \int \cdots \int \lambda^{\epsilon}_{\theta_1, j_1}(z) \ldots \lambda^{\epsilon}_{\theta_1, j_{k-1}}(z) \kappa^{\epsilon}_{\theta_1, t, j_0}(z) dz d\theta_1 dt \tag{9}$$

$$\leq \sum_{j_0} \sum_{0 \leq j_1 \leq \cdots \leq j_{k-1}} \int \cdots \int \lambda^{\epsilon}_{\theta_1, j_1}(z) \ldots \lambda^{\epsilon}_{\theta_1, j_{k-1}}(z) ||\kappa^{\epsilon}_{\theta_1, t, j_0}(z)||_\infty dz d\theta_1 dt.$$

And we have

$$||\kappa^{\epsilon}_{\theta_1, t, j}||_\infty \lesssim ||\beta_j||^2_{L^2(\mu)} \tag{10}$$

where $d\beta(x) = \sigma^{\epsilon}_t * \mu(x) d\mu(x)$.

Let ψ be a smooth positive function such that $\psi \geq \hat{\rho}$ and $||\psi||$ is bounded. Such ψ exists because $|\hat{\rho}(x)| \leq C_N(1 + |x|)^N$ for some constant C_N and integer N. Then

$$||\beta_j||^2 \approx \int |\hat{\beta}_j(\epsilon)|^2 d\epsilon \approx \int |\hat{\beta}_j(\epsilon)|^2 \hat{\psi}(\frac{\epsilon}{2^j}) d\epsilon$$

$$\approx 2^{dj} \int \cdots \int \psi(2^j(x - x')) \sigma^{\epsilon}_t * \mu(x) \sigma_t * \mu(x') d\mu(x) d\mu(x')$$

$$\lesssim 2^{j(d-s)} ||\sigma^{\epsilon}_t * \mu||^2_{L^2(\mu)}.$$

According to Theorem 2.1 in [1], we have that $||\sigma^{\epsilon}_t * \mu||_{L^2(\mu)}$ is bounded when $s > \frac{d+1}{2}$. From the assumption we have $k \geq 4 > 2$ and $d \geq 2 > 1$. Then there is $(d-1)(k-2) > 0$, and

we get $\frac{dk-d+1}{k} > \frac{d+1}{2}$, so the result from [1] applies and for each i, the left-hand side of (10) is bounded by $2^{j_0(d-s)}$. Therefore, each j_0-th piece of (9) is

$$\lesssim 2^{j_0(d-s)} \sum_{0\le j_1\le\cdots\le j_{k-1}} \int\cdots\int \lambda^{\epsilon}_{\theta_1,j_1}(z)\dots\lambda^{\epsilon}_{\theta_1,j_{k-1}}(z)dzd\theta_1.$$

Using the Plancherel theorem, we estimate this by

$$\lesssim 2^{j_0(d-s)(1)} \sum_{0\le j_1\le\cdots\le j_{k-1}} \int\cdots\int \hat{\lambda}_{\theta_1,j_1}(z) * \cdots * \hat{\lambda}_{\theta_1,j_{k-3}}(z) * \hat{\lambda}_{\theta_1,j_{k-1}}(z)\cdot\hat{\lambda}_{\theta_1,j_{k-2}}(z)dzd\theta.$$

The support of $\hat{\lambda}_{\theta_1,j_1} * \cdots * \hat{\lambda}_{\theta_1,j_{k-3}} * \hat{\lambda}_{\theta_1,j_{k-1}}$ has scale $2^{j_1}+\cdots+2^{j_{k-3}}+2^{j_{k-1}} \sim 2^{j_{k-1}} > 2^{j_{k-1}-1}$, and the support of $\hat{\lambda}_{\theta_1,j_{k-2}}$ has scale $2^{j_{k-2}}$. Therefore, if $j_{k-1}-j_{k-3}\ge 2$, then $2^{j_{k-1}-1} > 2^{j_{k-2}}$ and

$$\int\cdots\int \hat{\lambda}_{\theta_1,j_1}(z) * \cdots * \hat{\lambda}_{\theta_1,j_{k-3}}(z) * \hat{\lambda}_{\theta_1,j_{k-1}}(z)\cdot\hat{\lambda}_{\theta_1,j_{k-2}}(z)dzd\theta_1 = 0$$

in this case.

If $j_{k-1}-j_{k-2}=1$, then by Cauchy-Schwarz

$$\begin{aligned}
&\left(\int\cdots\int \lambda^{\epsilon}_{\theta_1,j_1}(z)\dots\lambda^{\epsilon}_{\theta_1,j_{k-1}}(z)dzd\theta_1\right)^2\\
&\le \left(\int\cdots\int \lambda^{\epsilon}_{\theta_1,j_1}(z)\dots\lambda^{\epsilon}_{\theta_1,j_{k-3}}(z)\left(\lambda^{\epsilon}_{\theta_1,j_{k-1}}(z)\right)^2 dzd\theta_1\right)\\
&\cdot\left(\int\cdots\int \lambda^{\epsilon}_{\theta_1,j_1}(z)\dots\lambda^{\epsilon}_{\theta_1,j_{k-3}}(z)\left(\lambda^{\epsilon}_{\theta,j_{k-2}}(z)\right)^2 dzd\theta_1\right)
\end{aligned}$$

which reduces to the product of two integral with their largest two indices for λ equal. It follows that we only need to consider the case when $j_{k-1}=j_{k-2}$. Similarly, by the orthogonal property of Littlewood-Paley pieces, we only need to consider the case $j_0=j_{k-1}=j_{k-2}=j$

Thus, using (10), we have that (9) is

$$\begin{aligned}
&\lesssim 2^{j(d-s)} \sum_{0\le j_1\le j_2\le\cdots\le j_{k-3}\le j} \int\cdots\int \lambda^{\epsilon}_{\theta_1,j_1}(z)\dots\lambda^{\epsilon}_{\theta_1,j_{k-3}}(z)\left(\lambda^{\epsilon}_{\theta_1,j}(z)\right)^2 dzd\theta_1\\
&\lesssim 2^{j(d-s)}\sum_j \sum_{0\le j_1\le j_2\le\cdots\le j_{k-3}\le j} 2^{(j_1+\cdots+j_{k-3})(d-s)} \int\cdots\int \left(\lambda^{\epsilon}_{\theta_1,j}(z)\right)^2 dzd\theta_1\\
&\le 2^{j(d-s)}\cdot C\sum_j 2^{j(k-3)(d-s)} \iint \left(\lambda^{\epsilon}_{\theta_1,j}(z)\right)^2 dzd\theta_1
\end{aligned}$$

By Section 5 and Theorem 3.1 in [7], we can use the Wolff-Erdogan Theorem to get the following result:

$$\int\cdots\int \left(\lambda^{\epsilon}_{\theta_1,j}(x-\theta_1x')\right)^2 d\mu(x)d\mu(x')d\theta_1 \lesssim 2^{j(d-s)-j\gamma(s,d)}$$

where $\gamma(s,d)=s-1$ if $s\ge\frac{d+2}{2}$, and $\gamma(s,d)=\frac{d+2s-2}{4}$ if $\frac{d}{2}\le s\le\frac{d+2}{2}$.

It follows that (9) is

$$\lesssim \sum_j 2^{j(d-s)}2^{j(k-3)(d-s)}2^{j(d-s)}2^{-j\gamma(s,d)} = \sum_j 2^{j[(k-1)(d-s)-\gamma(s,d)]}.$$

If $k\ge 4$ and $d>2$ are true, then a simple computation shows that $\frac{dk-d+1}{k}\ge\frac{d+2}{2}$. Thus if $s>\frac{dk-d+1}{k}$, then $s>\frac{d+2}{2}$, which implies that $(k-1)(d-s)-\gamma(s,d)=(k-1)(d-s)-(s-1)<0$.

If $k\ge 4$ and $d=2$ are true, then $s>\frac{dk-d+1}{k}=\frac{2k-1}{k}>1=\frac{d}{2}$, which implies that $(k-1)(d-s)-\gamma(s,d)=(k-1)(2-s)-\frac{2+2s-2}{4}=2k-2-(k-\frac{1}{2})s$. Simple computation shows that we have $s>\frac{2k-1}{k}>\frac{2k-2}{k-\frac{1}{2}}$, which entails that $(k-1)(d-s)-\gamma(s,d)<0$.

3. Proof of Theorem 2

For $i = 1, 2$, let θ_i be rotations such that

$$r\theta_i(x^{j_1} - x^{j_2}) \in B(y^{j_1} - y^{j_2}, \epsilon)$$

for $t_{j_1 j_2}$ in G_i.

Suppose $r > 0$. Then we have

$$\int \nu_G^\epsilon(r\vec{t})\ d\nu_G(\vec{t}) = \int T_{G_1}^\epsilon(x) T_{G_2}^\epsilon(x)\ d\mu(x^1)...d\mu(x^{k+1})$$

$$\approx \epsilon^{-\binom{k_1}{2}-\binom{k_2}{2}} \int \cdots \int_{\substack{||y^i-y^j|-r|x^i-x^j||<\epsilon \\ for\ all\ i,j\ s.t.\ t_{ij}\in\mathcal{E}(G)}} \prod_{s=1}^{k+1} (d\mu(x^s)d\mu(y^s)).$$

For rotation θ_i, just like in the last section, λ_{r,θ_i} is defined to be a measure on $\mathbb{R}^d$ by

$$\int f(z)\ d\lambda_{r,\theta_i}(z) = \iint f(u - r\theta_i v)\ d\mu(u)d\mu(v)\ ,\ f \in C_0(\mathbb{R}^d).$$

It has total mass $||\lambda_{r,\theta_i}|| = \mu(E)^2$. Let $d\theta$ be the Haar probability measure on $O_d(\mathbb{R})$.

We have

$$\liminf_{\epsilon\to 0} \int \nu_G^\epsilon(r\vec{t})\ d\nu_G(\vec{t})$$

$$\approx \int \cdots \int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{k_1} \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2}\ d\mu(x)d\mu(y)d\theta_1 d\theta_2$$

$$= \int \cdots \int \left(\int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{k_1} d\theta_2\right) \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y).$$

Without loss of generality, we can assume $k_1 \geq k_2$.

By Cauchy-Schwarz, if k_1 is odd, then

$$\left(\int \cdots \int \left(\int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{k_1} d\theta_1\right) \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)$$

$$\cdot \left(\int \cdots \int \left(\int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right) d\theta_1\right) \cdot \int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\ d\mu(x)d\mu(y)\right)$$

$$\geq \left(\int \cdots \int \int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{\frac{k_1+1}{2}} d\theta_1 \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)^2.$$

Note, that the second term of the left-hand side of the above inequality corresponds to a star-like graph with 2 parts, so is bounded above by following exactly the same steps when we proving Theorem1 until the last step of that proof. Therefore,

$$\left(\int \cdots \int \left(\int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{k_1} d\theta_1\right) \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)$$

$$\gtrsim \left(\int \cdots \int \int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{\frac{k_1+1}{2}} d\theta_1 \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)^2.$$

If k_1 is even, we have

$$\left(\int \cdots \int \left(\int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{k_1} d\theta_1\right) \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)$$

$$\cdot \left(\int \cdots \int \int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\ d\mu(x)d\mu(y)\right)$$

$$\geq \left(\int \cdots \int \int \left(\lambda_{r,\theta_1}^\epsilon(y - r\theta_1 x)\right)^{\frac{k_1}{2}} d\theta_1 \left(\int \left(\lambda_{r,\theta_2}^\epsilon(y - r\theta_2 x)\right)^{k_2} d\theta_2\right)\ d\mu(x)d\mu(y)\right)^2.$$

Again, the second term of the left-hand side of above inequality corresponds to a star-like graph with 2 parts, so is bounded above because of the same reason in the odd case. Therefore,

$$\left(\int\cdots\int\left(\int\left(\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_1 x)\right)^{k_1}d\theta_1\right)\left(\int\left(\lambda^{\epsilon}_{r,\theta_2}(y-r\theta_2 x)\right)^{k_2}d\theta_1\right)\,d\mu(x)d\mu(y)\right)$$
$$\gtrsim\left(\int\cdots\int\int\left(\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_1 x)\right)^{\frac{k_1}{2}}d\theta_1\left(\int\left(\lambda^{\epsilon}_{r,\theta_2}(y-r\theta_2 x)\right)^{k_2}d\theta_2\right)\,d\mu(x)d\mu(y)\right)^2.$$

Using the above process repeatedly, we get

$$\int\cdots\int\left(\int\left(\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_i x)\right)^{k_1}d\theta_1\right)\left(\int\left(\lambda^{\epsilon}_{r,\theta_2}(y-r\theta_2 x)\right)^{k_2}d\theta_2\right)\,d\mu(x)d\mu(y)$$
$$\gtrsim\left(\int\cdots\int\left(\int\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_1 x)d\theta_1\right)\left(\int\left(\lambda^{\epsilon}_{r,\theta_2}(y-r\theta_2 x)\right)d\theta_2\right)\,d\mu(x)d\mu(y)\right)^{2^m} \tag{11}$$
$$=\left(\int\cdots\int\left(\int\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_1 x)d\theta_1\right)^2\,d\mu(x)d\mu(y)\right)^{2^m}$$

for some integer m, where m is the number of doing the above process. By Cauchy-Schwarz, this is

$$\geq\left(\int\cdots\int\lambda^{\epsilon}_{r,\theta_1}(y-r\theta_1 x)d\theta_1\;d\mu(x)d\mu(y)\right)^{2^{m+1}}.$$
$$=\left(\int\cdots\int\lambda^{\epsilon}_{r,\theta_1}(z)d\theta_1\;dz\right)^{2^{m+1}}=\mu(E)^{2^{m+1}}$$

where E is a 2-chain.

Therefore for all $r>0$, (4) holds. This completes the proof.

References

1 Bennett M., Iosevich A. and Taylor K. Finite Chains Inside Thin Subsets of $\mathbb{R}^d$ // Analysis & PDE. -2016. -Vol. 9. No. 3. -P. 597–614.

2 Chatzikonstantinou N., Iosevich A., Mkrtchyan S. and Pakianathan J. Rigidity, graphs and Hausdorff dimension. Combinatorial and Additive Number Theory IV, 73–106. Springer International Publishing, cham, 2021.

3 Eswarathasan S., Iosevich A. and Taylor K. Fourier integral operators, fractal sets and the regular value theorem// Advances in Mathematics. -2011. -Vol. 228. -P. 2385–2402.

4 Falconer K.J. On the Hausdorff dimensions of distance sets//Mathematika. -1985. -Vol. 32. No. 2. -P. 206-212.

5 Gelfand I. and Shilov G. Generalized Functions. Academic Press. -1958. -Vol. 1.

6 Greenleaf A., Iosevich A. and Mkrtchyan S. Existence of similar point configurations in thin subsets of $\mathbb{R}^d$ // Math. Z. -2021. -Vol. 297. -P. 855-865.

7 Greenleaf A. , Iosevich A., Liu B. and Palsson E. A group-theoretic viewpoint on Erd ö s-Falconer problems and the Mattila integral// Revista MatemΓΫtica Iberoamericana. -2013. -Vol. 31. No 3. -P. 799–810.

8 Herz C. Fourier transforms related to convex sets// Ann. of Math. -1962. -Vol. 75. No 1. -P. 81-92.

9 Iosevich A. and Taylor K. Finite trees inside thin subsets of $\mathbb{R}^d$. Modern methods in operator theory and harmonic analysis, 51-56, Springer Proc. Math. Stat., **291**, Springer, Cham, 2019.

10 Iosevich A., Mourgoglou M. and Taylor K. On the Mattila-Sjolin theorem// Annales Academiae Scientiarum Fennicae. -2012. -Vol. 37. No 2. -P. 557–562.

11 Iosevich A. and Senger S. Sharpness of Falconer's $\frac{d+1}{2}$ estimate// Ann. Acad. Sci. Fenn. Math. -2016. -Vol. 41. No 2. -P. 713-720.

12 Mattila P. and Sjolin P. Regularity of distance measures and sets// Math. Nachr. -1999. -Vol. 204. -P. 157-162.

13 Sogge C. Fourier integrals in classical analysis. Cambridge University Press, 1993.

14 Stein E.M. Harmonic Analysis. -Princeton University Press, 1993.

15 Szemeredi E. and Trotter W. Extremal problems in discrete geometry//Combinatorica. 1983. -Vol. 3. No. 3-4. -P. 381-392.

16 Wolff T. Lectures on harmonic analysis Edited by Laba and Carol Shubin. University Lecture Series, Vol. 29. American Mathematical Society, Providence, RI, 2003.

А. Иосевич, С. Мкртчян, Т. Шен
Рочестер университеті, Нью-Йорк, 14627, АҚШ

Жабық нүкте конфигурациялары және Хаусдорф өлшемілігі

Аннотация: Мақалада $d(d \geq 2)$ өлшемді R^d жиынының компактты E жиыншасының хаусдорфтік өлшемділігі жетерліктей үлкен және G - әрбір бөлігі қатаң граф болатын екі бөлікті жұлдызды граф болғанда, граф арқылы берілген E-дегі қашықтықтар жиынының сәйкес өлшемділікті Лебег өлшемі оң болатыны дәлелденді. Сонымен қатар, $dim_H(E)$ жетерліктей үлкен болғанда

$$\int \nu_G(r\vec{t})d\nu_G(\vec{t}) > 0$$

теңсіздігі орындалатыны дәлелденді. Мұндағы ν_G – G-де анықталған қашықтықтар кеңістігіндегі Фростмен өлшемі арқылы индукцияланған өлшем. Дербес жағдайда, бұл дегеніміз кез келген $r > 0$ үшін $r\vec{t}$ төбелері де E жататын $(\vec{t})$ кодталған, төбелері де E-де жататын конфигурациялар жиыны табылады.

Түйін сөздер: ақырлы нүктелі конфигурациялар, топтық амалдар, симплекстер, Хаусдорф өлшемілігі.

А. Иосевич, С. Мкртчян, Т. Шен
Рочестерский университет, Нью-Йорк, 14627, США

Конфигурации закрытой точки и Хаусдорфова размерность

Abstract: В статье доказывается, что если хаусдорова размерность компактного E подмножества R^d с размерностью $d \geq 2$ достаточно велика, и если G есть звездный граф с двумя частями и каждая из его частей является жестким графом, то мера Лебега в соответствующей размерности набор расстояний в E, заданный графом, является положительной. Также доказано, что если $dim_H(E)$ является достаточно велико, то

$$\int \nu_G(r\vec{t})d\nu_G(\vec{t}) > 0,$$

где ν_G есть мера на пространстве расстояний, заданном G, которая индуцирована мерой Фростмена. В частности, это означает, что для любого $r > 0$ существует множество конфигураций, закодированных $(\vec{t}) >$ с вершинами в E, так что вершины $r\vec{t}$ также находятся в E.

Keywords: конечноточечные конфигурации, групповые действия, симплексы, хаусдорфова размерность.

References

1 Bennett M., Iosevich A. and Taylor K. Finite Chains Inside Thin Subsets of $\mathbb{R}^d$, Analysis & PDE. 2016. Vol. 9. No. 3. P. 597–614.
2 Chatzikonstantinou N., Iosevich A., Mkrtchyan S. and Pakianathan J. Rigidity, graphs and Hausdorff dimension. Combinatorial and Additive Number Theory IV, 73–106. Springer International Publishing, cham, 2021.
3 Eswarathasan S., Iosevich A. and Taylor K. Fourier integral operators, fractal sets and the regular value theorem, Advances in Mathematics. 2011. Vol. 228. P. 2385–2402.
4 Falconer K.J. On the Hausdorff dimensions of distance sets, Mathematika. 1985. Vol. 32. No. 2. P. 206-212.
5 Gelfand I. and Shilov G. Generalized Functions. Academic Press. 1958. Vol. 1.
6 Greenleaf A., Iosevich A. and Mkrtchyan S. Existence of similar point configurations in thin subsets of $\mathbb{R}^d$, Math. Z. 2021. Vol. 297. P. 855-865.
7 Greenleaf A. , Iosevich A., Liu B. and Palsson E. A group-theoretic viewpoint on Erd ö s-Falconer problems and the Mattila integral, Revista MatemГЎtica Iberoamericana. 2013. Vol. 31. No 3. P. 799–810.
8 Herz C. Fourier transforms related to convex sets, Ann. of Math. 1962. Vol. 75. No 1. P. 81-92.
9 Iosevich A. and Taylor K. Finite trees inside thin subsets of $\mathbb{R}^d$. Modern methods in operator theory and harmonic analysis, 51-56, Springer Proc. Math. Stat., **291**, Springer, Cham, 2019.
10 Iosevich A., Mourgoglou M. and Taylor K. On the Mattila-Sjolin theorem, Annales Academiae Scientiarum Fennicae. 2012. Vol. 37. No 2. P. 557–562.
11 Iosevich A. and Senger S. Sharpness of Falconer's $\frac{d+1}{2}$ estimate, Ann. Acad. Sci. Fenn. Math. 2016. Vol. 41. No 2. P. 713-720.
12 Mattila P. and Sjolin P. Regularity of distance measures and sets, Math. Nachr. 1999. Vol. 204. P. 157-162.
13 Sogge C. Fourier integrals in classical analysis. Cambridge University Press, 1993.
14 Stein E.M. Harmonic Analysis. Princeton University Press, 1993.
15 Szemeredi E. and Trotter W. Extremal problems in discrete geometry, Combinatorica. 1983. Vol. 3. No. 3-4. P. 381-392.
16 Wolff T. Lectures on harmonic analysis Edited by Laba and Carol Shubin. University Lecture Series, Vol. 29. American Mathematical Society, Providence, RI, 2003.

Information about authors:
Алекс Иосевич – ***Байланыс үшін автор***, Рочестер университетінің профессоры, Нью-Йорк, 14627, АҚШ.
Севак Мкртчян – Рочестер университетінің профессоры, Нью-Йорк, 14627, АҚШ.
Тритий Шен – Рочестер университетінің профессоры, Нью-Йорк, 14627, АҚШ.
Alex Iosevich – ***Corresponding author***, Professor, Department of Mathematics, University of Rochester, Rochester, NY, 14627, USA.
Sevak Mkrtchyan – Professor, Department of Mathematics, University of Rochester, Rochester, NY, 14627, USA.
Tritium Shen – Graduate Student, Department of Mathematics, University of Rochester, Rochester, NY, 14627, USA.

Received 15.03.2022

Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2022, Vol. 138, №1, P.45-54
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

IRSTI: **27.21**

Ғ.Е. Тауғынбаева [1] , А.Ж. Жұбанышева [2] , Ж.Қ.Табылдиева [3] , Н.Темірғалиев [4]

[1,2,4] *Л.Н.Гумилев атындағы Еуразия ұлттық университетінің Теориялық математика және ғылыми есептеулер институты (ТМ және ҒЗИ), Сәтпаев көш., 2, НұрСұлтан, 010008, Қазақстан*

[3] *Бауыржан Момышұлы атындағы № 46 орта мектеп, Жаңа Орда, 30, Орал, Қазақстан (E-mail:* [1] *galija_1981tau@mail.ru,* [2] *zhubanysheva_azh@enu.kz,* [4] *ntmath10@mail.ru)*

Бастауыш мектептегі сан және оған қолданылатын қосу және көбейту амалдарын оқыту әдістемелері мен соның төңірегіндегі жалпы мәселелер

Аннотация: Нәтижесінде «Математикалық кемелдену» деңгейіне жеткізу үшін заманауи Жасанды интеллекттің жалпы идеялары негізіндегі сандар, оларға қолданылатын қосу және көбейту амалдары тақырыптарын беруде тікелей қолданыстағы әдістеме мен бастауыш мектепте «Көбейту кестесін» өз бетінше құру әдістемесі ұсынылады.

Түйінді сөздер: Ауызша санау, санды хатқа түсіру, сандарды қосу, сандарды көбейту, сандардың орынауыстырымдылық қасиеті, көбейту кестесі.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.4

2000 Mathematics Subject Classification: 97F30, 00A35, 97F10.

1. «Математикалық кемелдену» дегеніміз не және ол дәрежеге оқушы қалай жеткізіледі? Мектеп математикасындағы басты мақсат – бірінші сыныптан бастап, соңғы сыныпқа дейін бірте-бірте оқушыны мектеп бітіргенде «Математикалық кемелдену» атты (дәл анықтамасы жоқ, бірақ бар-жоғы аңқып тұрады) деңгейге жеткізу болып табылады.

Математикалық (тек бұнда ғана емес) білім беру мұғалімнің оқушыға дұрыс сөздер мен сөйлемдерді жалаң айтып беруі мен дайын формулаға қойып есеп шығарудан емес (жиі кездесетін оқытуға жарамсыз оқулықтар жағдайында бұл да жетістік қатарына жатса да), әрдайым толық математикалық заңдылықтармен дәлелдеу жүргізу арқылы, ал бұл мүмкін емес болған жағдайда толық логикаға сай дәлелдемені бермесе де, соған жанасатын түсіндірмеден құрылуы керек. Осының негізінде әрқашанда мәселе-есеп қойылымын, оның қалай шығарылып жатқанын, нақтылы дәлелдеулер қалай жүріп және неге дәлелдеп жатқанын дұрыс түсінетін деңгейге дейін жеткізу қажет деген ұстанымда болуы міндетті, әрқашан да әр тақырыпта әйтеуір қандай да бір түсіндірме болуы керек! Әрине, күнделікті өмір қажеттілігінен туындаған, қарапайымнан аса күрделіге дейін жалғасып жатқан математика ғылымының ауқымының аса кеңдігі мен өмірге жақындығы мектеп математикасында дәлелдеу жүргізуге мүмкіндік береді. Қорытындысында, білім алушыдан қойылған есеп жайлы сұрағанда оның сандық жауабын ғана емес, сол есепке қатысты бүкіл математикалық құрылымды түсініп айта алуы қажет, – дәл осы «Математикалық кемелденуге» әкелетін жол не сондай жолдардың бірі болып табылады.

Оқу жасындағы баланың өзгеріп отыратын заманына және жас ерекшелігіне қарай дәл қазір бөлшек, логарифм тәрізді барлық тақырыптарды қашан және қалай беру керектігін анықтаудың ТМ және ҒЗИ ұсынған авторлық әзірлемелері бар. Ол әдіс бойынша зерттелінді әр тақырыптың мазмұны Қазақстанның барлық аудандарындағы әр жастағы оқушылардан тұратын топтарға бір сабақ деңгейінде қысқа түрде толық беріледі де, сол бойынша бала тақырыпты қандай деңгейде игергендігіне әртүрлі жолдармен талқылаулар жүргізілу нәтижесінде қай жаста осы тақырыпты беруге болатындығы зерттеліп, бүкіл

Қазақстан бойынша жинақталған мәліметтерден толық оқу мерзіміне арналған бір-бірімен сабақтасқан бірыңғай Оқу бағдарламасы құрылады (толығырақ [1]-ді қараңыз).

2. Мақала мақсаты мен мазмұны. Бұл мақала күнделікті өмірде, ғылым мен техникада қолданылатын, ғылымның негізі болып табылатын сан ұғымының мағынасы мен оның цифр арқылы жазылуына, қосу және көбейту амалдары тақырыбына арналған, ол жоғарыдағы ұстанымдарға сай беріледі және тақырыпты беру барысында ыңғайына қарай ұстаным қай жерде, қалай қолданылып отырғандығы да көрсетіледі.

3. Мектеп математикасы біртұтас, кез келген жерінен нәтижелі кіре алмайтындай ерекше жүйеленген Білім әлемі. Математика білімі – жүйелендірілген білім, ал мектеп аясындағы жүйелендіру дегеніміз тек осы ғылымның ең басы болатын саннан, бір-бірімен байланыстыра отырып, кішкентай баспалдақтар жолын бастауыш мектептен бастап, соңғы сыныпқа дейін жүріп өту дегенді білдіреді. Дәл осы жүйелендіру күмән тудырған сәттерде қандай да бір дәлелдеу не математикалық қатаң дәлелдеуге келмесе де, шындыққа жанасатын талқылаулармен көз жеткізуге мүмкіндік бере алатын сенімді білімге, яғни «Математикалық кемелденуге» алып келеді. Кейбір пәндердің алдыңғы бөлігін игермей-ақ, кез келген тақырыбынан бастап немесе ортасынан бірнеше тақырыпты тастап кетіп, басқа бір бөлігінен бастап, келесісін түсіндіруге болса, орта мектеп математикасында ондай мүлдем болмайды, математикалық білімде бірде-бір тақырып қалмай, бірінен кейін бірі бала санасына, артынша түпсанасына бірте-бірте сіңуі қажет.

4. Он бір жылдық ұзақ Математикалық жолдың сан ұғымынан басталуы. Бұл жол сан мен оларға қолданылатын амалдарды, қасиеттеріне қатысты ережелерді төбеден түскендей жаттатыра салмай, мағынасымен түсінетін деңгейге жеткізуден басталады. Бұл жолдағы басты тірек – мектепке келген бала тіл грамматикасын білмей-ақ дұрыс сөйлей алғаны сияқты математика құрылысын білмей-ақ ауызша «Бір, екі, үш, ...» түрде санай алуы. Бала ауызша сөйлей алғанымен оған әліппе арқылы әріп атты А,Ә,...,Ю,Я таңбаларды танытып, ары қарай қазақ тілі грамматикасын үйреткендей, ауызша санай алатын балаға да бірінші сыныпта әріптің математикадағы міндетін атқаратын, әріпке қарағанда «*орындық*» ерекшелігі бар цифр атты 0,1,2,3,4,5,6,7,8,9 таңбалармен санды хатқа түсіртіп, арифметика атты санға қолданылатын қосу, алу, көбейту, бөлу амалдары мен олардың қасиеттерін зерттейтін математика саласын, ары қарай Оқу бағдарламасына енетін математиканың барлық тақырыптарын игертеді.

5. Қоғамда өскен баланың оқусыз-ақ ауызша санауды үйренуі ғажайып құбылыс екендігін IT-қауымы ертерек түсінсе, «Жасанды интеллект» жетістігін әлдеқашан ілгері әрі ауқымды жылжытуға мүмкіндік көзі болатындығының осы жерде көрінуі. Компьютерді «Адам миы» деңгейіне жеткізу мақсатында адам миы қазіргі күнге дейін қарқынды зерттеліп келе жатқанымен, теориясы жасалған, бірақ техникалық тұрғыдан іске асыру мүмкін емес болып отырған, жалпылап айтқанда, санның орнына матрица қолданылатын «Кванттық компьютерді» құралмаған тәрізді, «Адам миы» деңгейіндегі құрылғыға да қол жеткізу әлі де күмәнді жағдайда қалып отыр.

Осы тұрғыда баланың жас ерекшелігіне байланысты дамуына қарай 2-3 жасқа келгенде еш грамматиканы білместен, қоршаған қоғам әсерінен дұрыс сөйлеуді үйренетіндігі жайлы сөз қозғалған еді. Бұндағы «грамматиканы білмей-ақ» деген сөз тіркесінің мағынасын бір қарағанда жылдам әрі дұрыс аударып беретін аудармашы тұрғысынан талқылайық: бір тілден екінші тілге мәтін аударғанда компьютер жеке-жеке сөздердің аудармасын орын-орнына қойып шыққанымен, сол сөздерден аударылып жатқан тілдің грамматикасын қолданып, сөйлем құруға қаншама әрекет жасалса да, іс жүзінде қолдануға жарамды нәтижеге әкелмей қойды. Оның шешімі жадыға көп көлемде (қоғамдағы адамдардың сөйлеуі сияқты) дұрыс аударылған мәтіндерді жинақтап, берілген мәтінге ұқсас мәтіндерді тауып (әрине, бұл компьютер қуаты қажетті деңгейге жеткенде ғана мүмкін), солар арқылы «Машиналық оқыту» атты математиканың жаңа бағыты бойынша тәжірибелі аудармашының қателігінен де төмен қателікпен жүзеге асырылады. Баланың сөйлеуді үйренгеніне басқаша – күнделікті қоғамнан дұрыс сөйлемдерді ести жүре өзі солардың арасынан таңдау жасау алгоритімі деп қарайтын болсақ, қарастырылып отырған аударма

мәселесі бұрынырақ шешілер еді және осыны тек аударма ғана емес, «Жасанды интеллект» пен «Машиналық оқыту» салаларындағы кез келген мәселеге қатысты да айтуға болады.

Жалпы, «Машиналық оқыту» бағыты «Жасанды интеллекттің» бір бөлігі деген түсінік қалыптасқан, бірақ олардың мазмұндары әлі де тұрақталмағандықтан кейбір мамандардың пікірі бойынша олар синоним атаулар деп те саналады. Қалай болғанда да бұндағы «машина» деген компьютер, ал біз қарастырып отырған жағдайда өзара бөлек сөйлеу құралдарын, санауды сол компьютерге түсіруден тұратын *«мұғаліммен машиналық оқыту»* атты үрдіс мұғалімнің рөлін қоғам атқарғандағы *«Ұстазбен оқу»* түріндегі «баланың айналасынан» есту арқылы сөйлеп, санап үйренетін бала миының моделі.

Сондай-ақ, 3-4 жасар бала әртүрлі тұқымдағы ит пен мысықты бір-бірінен оңай ажырата алса, «Жасанды интеллект» үшін бұл да өте күрделі мәселе.

Сандармен де жағдай тура осындай, бала әртүрлі заттарды танып, бір-бірінен ажыратуды үйренгендей, ешқандай грамматиканы білмей-ақ сөйлеп үйренгендей, математикалық заңдарсыз-ақ күрделі болып табылатын *санақты* үйренеді.

6. «Сан деген не?» сұрағына Математика ғылымы әлеміндегі «Сан деген логика!» жауабын бастауыш мектеп деңгейіне келтіру жолы. Осы тұрғыда бізге қажетті «Натурал сандар тізбесі» деп аталатын 1,2,... сандарына көшелік. Оқушы мектепке дейін-ақ жазылуы бірдей, бірақ мағынасы бойынша әртүрлі – айналасындағы заттардың санын «Бір, екі,...» білу мақсатындағы *сандық* және ретін көрсететін «Бірінші, екінші, ...» *реттік* сандарды біледі деп қабылданады. Жоғарыда айтқандай, бала сөйлеу құралы – сөздерді грамматикалық ережесіз игергендей, өте терең сан ұғымын оң бүтін сандарды толық беретін аксиомалар ережелердің жинағынан құралған Пеано, саны бірдей заттардың барлығына бір ортақ белгі сәйкес қою арқылы санды анықтайтын Фреге-Рассел ережелер аксиомаларын білмей-ақ «Нөл, бір, екі, үш, ...» сандар тізбесін мектепке енді келген бала жасы деңгейінде меңгереді. Осы айтылғандарды қорытындылай келе *«Бала сандық және реттік санауды біледі»* деген тұжырымды негізге аламыз.

7. Сандардың цифр атты таңбалармен, ал сөздердің сол дәрежедегі әріптаңбалармен жазылуы және сол жазуларда цифрдің әріпке қарағанда орындық мағынасы. Күнделікті сөйлеп жүрген сөздерін әліппенің әріптері арқылы жазуға үйреткендей мектеп математика бағдарламасы ауызша санай алатын сандарды хатқа түсіруден басталады. Дәл дыбыстарды жазуға арналған әріп белгілеулері тәрізді сандарды белгілеу үшін де цифр деп аталатын арнайы белгілеулер қолданылады. Санды жазуға қолданылатын белгілердің саны *санақ жүйесін* анықтайды, олардың ішінде кең таралғаны 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 цифрлерін қолданатын *ондық санақ* жүйесі.

Қазақ тілі грамматикасында сөздерді жазу барысында әріп қай жерде тұрса да, өзгеріссіз бір ғана дыбысталуда болғанымен, мәселен, «Алима» сөзінде екі рет кездесетін «А» әрпі әртүрлі жерде тұрса да, дыбысталуы бірдей, ал санды жазудағы цифр өзінің мәндікпен қоса орындық та (бұны «позиция» деп те атайды, латын тілінде *positio* — орны, жағдайы, орналасқан жері) қызметін атқарады. Мысалы, 777 натурал санының жазылуындағы 7 цифрі, «жеті» деген мағынасымен қоса, оңнан солға қарай жүргенде біріншісі жеті бірлік барын, екіншісі жеті ондық барын және соңғы үшіншісі жеті жүздік барын білдіреді:

$$777 = 7 \cdot 100 + 7 \cdot 10 + 7 \cdot 1 = 7 \cdot 10^2 + 7 \cdot 10^1 + 7 \cdot 10^0.$$

жалпы жағдайда

$$a_k a_{k-1} ... a_1 a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

мұндағы $a_0, a_1, \ldots, a_k$ - цифрлер.

Бұндай жазуды *позициялық жазу* деп атайды (толығырақ [2-3] қараңыз).

8. Сандарды таяқшалар жинағы арқылы бейнелеу және керісінше, таяқшалар тізбесінен олардың санын шығарып алу. Тақырыптарды сызуға оңай және нақты «таяқшалар» не математика тілінде айтқанда «сызықшалар» көмегімен оқушыға көрнекі түрде түсіндіретін Теориялық математика және ғылыми есептеулер

институтының өз авторлық әдістемесі бар [4]. Кейбір мектептерде таяқшаның орнына шеңбер, нүкте де қолданылып жатады, бірақ шеңберді сызу күрделі болса, ал нүктені қадағалап отырмаса, көрінбей де қалуы мүмкін.

$\underset{1}{|}$ болғандықтан 1-дегенге $|$ таяқша саламыз, 2 – санының орнына $||$, өйткені $\underset{1\,2}{|\,|}$, дәл осы сияқты таяқшалармен *санақ* жүргізіледі.

Жалпылап айтқанда, «бала ауызша санай алады» деген ұстанымымызды негізге алып, таяқша сыза бастағаннан әр таяқшаны саната отырып, қажетті санға келгенде сызуды тоқтата қою арқылы (дәл осыны мүдіртпей орындау керек екендігіне ерекше көңіл аударамыз!) әр сан қанша таяқшамен бейнеленетіндігін және керісінше, сызылып тұрған таяқшалар қандай санды білдіріп тұрғанын анықтата білу қажет.

9. Математикалық білімнің дұрыс жауапты ғана емес, тіпті «құрғақ» дәлелді де ғана емес, айтылғандардың мән-мазмұнын «ішпен сезіп, бойға сіңіргендей» түпсана деңгейінде болу керектігі, сонымен «Математикалық кемелдену» деңгейін қамтамасыз етуі – сандарды қосу амалының дәлелді оқыту әдістемесі. Сандарды жазу тәртібін игерді деп есептеп, оларға қолданылатын қосу және көбейту амалдарына көшелік. Әртүрлі екі жәшікте тұрған сандары белгігі ойыншықтарды бір үлкен жәшікке жинағанда барлығы қанша ойыншық болатындығын табу керек деген есеп қойылымы «қосу» деп аталатын амалға алып келеді. Мәселен, жәшіктердің бірінде 3, екіншісінде 2 ойыншық бар болса, онда жинақталған ойыншықтар санын анықтауда «+» таңбасы енгізіліп, саны 3+2 жазуы арқылы белгіленеді. Бұнда жеке-жеке жәшіктердегі ойыншық сандары болатын екі санға қосу амалы қолданылғанда «*қосылғыштар*» деп, ал біріктіріп санағанда шыққан ойыншықтардың жалпы санын беретін – бір сан «*қосынды мәні*» деп аталады.

Әрине, мұғалімнің «3+4 не болады?» деген сұрағына мағынасына мән бермей, тек есептеуді ғана үйреніп алған көптеген баладан дұрыс, әрі тез 7 деген жауап алады, өкінішке орай ата-ана да, мұғалім де осыған қанағаттанып, тіпті қуанып, баланы мақтап жатады. Ұстанымызға сәйкестендіріп, қосу амалының жүйелі түріне көшейік.

Бірақ, білім сенімді болуы керек, сондықтан балаға ары қарай «Жоқ, 7 емес, менің жауабым 8 немесе 9» деп, баланың өз жауабын дұрыс екендігін дәлелдеуге, ол арқылы қосу амалының мағынасын түсінуге алып келу қажет.

Сандарды таяқшалар арқылы жаза және таяқшадан санға көше алғаннан кейін ғана 2+2 амалын орындауға дайын боламыз: Алдымен 2 санына сәйкес санай отырып, $||$ таяқша саламыз (және таяқшалар саны екіге жете салысымен тоқтаймыз), «+» таңбасынан кейін дәл осы әдіспен тағы 2 санын таяқшалар жинағымен бейнелейміз, қосу амалынсыз таяқшаларды қатар жаздырып алып, осы таяқшаларға жалпы санақ жүргіздіртіп, керісінше таяқшалар жинағынан санға көшеміз, нәтижесінде 4 шығатындығын бала өз қолымен дәлелдеп, көз жеткізеді

$$2+2=\underset{1\,2}{|\,|}+\underset{1\,2}{|\,|}=||||=\underset{1\,2\,3\,4}{|\,|\,|\,|}=4.$$

Дәл осы сияқты

$$2+3=\underset{1\,2}{|\,|}+\underset{1\,2\,3}{|\,|\,|}=|||||=\underset{1\,2\,3\,4\,5}{|\,|\,|\,|\,|}=5.$$

Жалпылап айтқанда, қосылғыш болатын екі сан жазылады да, келесі қадамда сол сандар сәйкес таяқшалар жинағымен бейнеленеді, артынша оларды жәшіктердегі ойыншықтарды қосып жібергендей араластырып бірге жазып аламыз, одан кейін барып, керісінше, таяқшалардан санға көшу үрдісімен, бастапқы екі санның қосындысы болатын қосынды мәні атты бір санға келеміз.

Математикада жазуға ерінбеу негізгі қағиданың бірі болып табылады, сондықтан да қосу таңбасын алып тастап, бір жаздырып, артынан цифрлармен белгілей отырып екінші рет жаздыртып негізгі нәтижеге жетуді бірнеше мысалдармен баланың бойына сіңдіру қажет, сонда ғана ол өзіне де, күмән келтірген адамдарға да кез келген уақытта толық дәлелдей алады.

Әрине, бұл әдіс балаға қосу амалының затын түсіндіру мақсатында қолданылады да, кейін есептеу таяқшасыз-ақ жүргізіле береді.

10. Қосу амалының орын ауыстырымдық қасиетінің математиканы оқыту үстіндегі қаупі және одан арылу жолы. Келесі кезекте қосу амалының «*Қосылғыштардың орнын ауыстырғанда қосындының мәні өзгермейді*» деп тақпақ тұрғысынан жаттаумен шектеліп жүрген ауыстырымдылық атты $a + b = b + a$ қасиеті. Мектеп математикасы бағдарламасының дәл осы жері бала үшін өте қауіпті, бір қарын майды шірітетін бір құмалақ тәрізді бұл да математиканы игеру жайлы жалған түсінік тудырады. Мұғалімнің айтқанын жаттап алып, өзіне дәлме-дәл қайталап айту мектеп математикасын игеру жолында оқушы санасына «*жаттап алсаң болды*» деген жалған түсінік тудыратын қауіпті жағдайға жатады – әрқашан да дәл дәлелдеме, қала берді қандай да болсын негіздеме міндетті түрде болуы керек!

a және b сандары екі ретте бола алады, бірінші a, екінші b, онда олардың қосындысы деп аталатын $a + b$ түрінде белгіленетін сан, ал керісінше b саны бірінші, a саны екінші болғанда $b + a$ түріндегі сан сәйкес қойылады. Кейбір құнды математикалық құрылымдарда қосындысы болып отырған $a + b$ және $b + a$ сандары тең болмауы да мүмкін, сондықтан дәл сандар үшін олардың өзара тең болуы ерекше назар аудартады. Бұл қасиет үлкен математикадағы топ деген математикалық құрылымда кеңінен талқыланады, мектеп мұғалімінің өзі оқушыға еркін айтуы үшін осы тақырыпты жітік меңгеруі міндетті болғанымен оқушыға мұны түсіндіру мүмкін де емес, керек те емес!

Енді $a+b=b+a$ қасиетін бастауыш мектеп қабырғасы деңгейінде негіздеу әдістемесіне тоқталайық. Мектеп математикасында заң деп ауыз толтырып айтылатын $2 + 3 = 3 + 2$ теңдігі 6-8 жастағы қосуды үйренген бала үшін – бір қолына 2 конфет, екіншісіне 3 конфет алады да, алдымен қолдарын бір-біріне параллель созады, артынша айқастырады да, айтады: «Ештеңе өзгерген жоқ, барлығы бәрі-бір 5 конфет».

Мектеп математикасында жас ерекшеліктеріне байланысты дәлелдеу мүмкін емес болатын жағдайлар «шындыққа жақын» деңгейде бәрі-бір түсіндірулі қажет екендігі жоғарыда айтылған еді, сол ұстанымды қосудың ауыстырымдық қасиеті мысалында жандандырайық.

Оны да «таяқшалар» әдісі арқылы саннан таяқшаға, таяқшадан санға көшу бойынша жүзеге асыруға болады, сонымен $2 + 3 = 3 + 2$ теңдігін санау мен қосу амалын енді үйренген балаға арналған негіздеуін ұсынайық. Ол үшін алдымен таяқшалар тілінде 2+3 амалы орындалады:

$$2+3 = \underset{1\,2}{|\,|} + \underset{1\,2\,3}{|\,|\,|} = \underset{1\,2\,3\,4\,5}{|\,|\,|\,|\,|} = 5,$$

артынша дәл сол тұрған қалпында алынған 5 таяқшаны басқаша – алдымен 3 таяқшаны бір бөліп алып, одан кейін қалған 2 таяқшаны бір топтастырып, оны санап алғаннан кейін таяқшалар жинағына сан сәйкес қою арқылы сандарға көшсек

$$\underset{1\,2\,3\,4\,5}{|\,|\,|\,|\,|} = \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2}{|\,|} = 3+2.$$

Бұл дәлелдеулерді біріктіріп,

$$2+3 = \underset{1\,2}{|\,|} + \underset{1\,2\,3}{|\,|\,|} = \underset{1\,2\,3\,4\,5}{|\,|\,|\,|\,|} = \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2}{|\,|} = 3+2$$

мақсатымыздағы $2 + 3 = 3 + 2$ теңдігінің тікелей дәлелдеуін аламыз.

Сонымен, алдымен 2 және 3 сандарының қосындысы 5 санына тең екендігін алғаннан кейін кері қарай таяқшаларды керегімізше (әрине топтастыруды әртүрлі жүргізуге болады, мысалы, 5 таяқшаны 4 және 1 таяқшалар жинағы түрінде де топтастыруымыз мүмкін, бірақ балаға топтастыру алынған қосылғыштаға сәйкес орындау керектігін баса айту қажет) топтастырғаннан кейін таяқшалардан санға көшу бойынша 5 саны 3+2 сандарының да қосындысы болғанын бала өзі қорытып шығара алады, тағы қажетінше мысалдарды дәл осы әдіспен үйреткеннен кейін ғана қайсысын бірінші қойсаң да бәрі-бір деп үйрету қажет.

Бір айтылғанды мүмкіншілігіне қарай басқа жолдармен де нақтылай беру оқыту әдістерінің бірі болып табылады, сол тұрғыда, көрнекі түрде осы қасиетті жәшіктердегі

ойыншықтар арқылы да беруге болады. Жоғарыда қосу амалын негіздегендегі жәшіктер ішіндегі ойыншықтардың қайсысын бірінші, қайсысын екінші үлкен жәшікке салсақ та, үлкен жәшіктегі ойыншықтар саны өзгермегендігінен ауыстырымдық қасиет негізделеді.

Ал үлкендер оны («мардымсыз ақылдың ашулы рухы!»): 2+3=3+2 және де жалпы айтқанда, a+b=b+a, бұл ауыстырымдылық заңы деп үйретеді. Бұл балаға еш түсініксіз, құрғақ сөйлемді жаттау қызметін атқарады.

11. Көбейту амалы – бірдей қосылғыштардың қосындысының үнемді, қысқа белгіленуі. Қосу амалын түсінгеннен кейін 4 теңге тұратын 3 дәптер алу үшін қанша теңге қажет екендігін есеп ретінде қояйық, оқушы 4 санын өз-өзіне 3 рет қосады, артынан осындай бірдей қосылғыштарды өз-өзіне бірнеше рет қосу арқылы *көбейту* деп аталатын жаңа амал енгізілетіндігін түсіндіру қажет. Ғылымдағы арифметикалық көбейту амалының «Үш көбейту төрт» оқылуының Ахмет Байтұрсынов енгізген бірден өзі амалдың мағынасын ашып тұрған «Үш жердегі төрт» оқылуы математикалық ішкі заңдылығын білдіретін «*3 × 4 дегеніміз не?*» және сандық сипатын білдіретін «*3 × 4 мәні неге тең?*» деген және де сол арқылы математиканы түсіну, түсінбеуін көрсететін екі сұраққа бөлінеді. Бұны «Математикалық кемелдену» жолындағы әбден түсініп алатын алғашқы құрылым деп қабылдау керек: Бірінші «*3 × 4 дегеніміз не?*» деген сұраққа жауап беруден, яғни көбейту амалының анықтамасынан бастайық, «Үш жердегі төрт» деген сөз тіркесі анықтаманың өзін толық беріп тұр десек те болады, үш жерде төрт-төрт таяқшадан тұр, солардың қосындысы 3 санын 4 санына көбейту деп аталады, яғни 3 × 4=4+4+4 деген 4 саны қосылғыш ретінде 3 рет алынады (4 саны 3 орында тұр). Арy қарай игерген қосу амалын таяқшалар арқылы орындасақ:

$$3 \times 4 = 4 + 4 + 4 = \underset{1\,2\,3\,4}{||||} + \underset{1\,2\,3\,4}{||||} + \underset{1\,2\,3\,4}{||||} = \underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{||||||||||||} = 12.$$

Бұл теңдік оқушыға *«3 × 4 мәні неге тең?»* деген екінші сұрақтың жауабы 12 санына тең екендігін де береді.

12.«Көбейту кестесі», оны өз қолымен құру әдістемесінің оқушыны алғашқы ғылыми нәтиже биігіне көтеруі. Көбейту кестесі деп *n=2,3,4,5,6,7,8,9* және *a=2,3,4,5,6,7,8,9* сандарының $n \times a$ (яғни, бір цифрмен жазылатын 2,3,4,5,6,7,8,9 сандары үшін) түріндегі көбейтінділерінің сандық мәндерінің *n=2,3,4,5,6,7,8,9* үшін жеке бағанамен берілген *кесте* түрінде жазылуы.

Мектепке дейінгі және бастауыш мектеп жасындағы балалар үшін санау таяқшаларының (немесе сіріңке сынды олардың алмастырулары) көмегімен көбейту кестесінің толық нұсқасын жасауды ұсынамыз. Бұл жағдайда үйретушіге (аға мен апасы немесе ата-анасына) баланы асықтырмау ұсынылады. Неғұрлым кішкентай болатын болса, соғұрлым асықтырмаған жөн. Әрбір бағанды толтырылған соң, өзіне деген сенімділігін арттыру және жаңа ізденістерге құлшыныс жасау үшін басылған дайын көбейту кестенің көшірмесін көрсету керек (мысалы, дәптердің сыртындағы).

Бірінші баған толтырғаннан кейін (ол кез келген тәртіппен ұсынылуы мүмкін, мәселен *n=3*-тен бастаса да болады, себебі түсіндірмелер 3 санымен жүргізілген) және дәптердің артында басылған көбейту кестесімен салыстыра, қатесі болса түзетіп болғаннан кейін, балаға бұл сенің өзің тұңғыш орындаған ғылыми жұмысың деп түсіндіру қажет, – әдетте «Жаттап ал!» деп жоғарыдан түскендей математикалық есепті өз қолымен шығарғаны бала үшін үлкен әсер қалдырады, балада «Математика менің де қолымнан келеді екен» деген сезім тудыралы, ал келесі бағандарды дәлеледеген кезде осы сезім бала бойында күшейе түсетіні анық.

«Көбейту кестесінің бір бағанын толтыру» тапсырмасының орындау барысын көрсетейік: алдымен көбейту амаланың анықтамасын келісім бойынша таңбалап аламыз, артынша анықтаманың атынан затына, яғни қосуға көшеміз. Қосу амалын өзіміз білетін таяқшалар әдісімен орындайтын болсақ, көбейтудің сандық мәніне келеміз.

$3 \times 1 = 1 + 1 + 1 = | + | + | = ||| = 3$

$3 \times 2 = 2 + 2 + 2 = || + || + || = |||||| = 6$

$3 \times 3 = 3 + 3 + 3 = ||| + ||| + ||| = ||||||||| = 9$

$3 \times 4 = 4 + 4 + 4 = |||| + |||| + |||| = |||||||||||| = 12$
$3 \times 5 = 5 + 5 + 5 = ||||| + ||||| + ||||| = ||||||||||||||| = 15$
$3 \times 6 = 6 + 6 + 6 = |||||| + |||||| + |||||| = |||||||||||||||||| = 18$
$3 \times 7 = 7 + 7 + 7 = ||||||| + ||||||| + ||||||| = ||||||||||||||||||||| = 21$
$3 \times 8 = 8 + 8 + 8 = |||||||| + |||||||| + |||||||| = |||||||||||||||||||||||| = 24$
$3 \times 9 = 9 + 9 + 9 = ||||||||| + ||||||||| + ||||||||| = ||||||||||||||||||||||||||| = 27$
$3 \times 10 = 10 + 10 + 10 = |||||||||| + |||||||||| + |||||||||| = |||||||||||||||||||||||||||||| = 30.$

13.Қайсысы қиынырақ және тезірек – қосу ма әлде көбейту ме? Көбейтудің анықтамасына сәйкес көбейтудің бір амалы

$2 \times a$ *қосудың 1 әрекетінен тұрады* $a + a$
$3 \times a$ *қосудың 2 әрекетінен тұрады* $a + a + a$
.....
$n \times a$ *қосудың* $n - 1$ *әрекетінен тұрады* $\underbrace{a + a + \cdots + a}_{n-\text{рет}}$

мұндағы n қосынды саны 5, 10, 1947 және қалауымыз бойынша алынған кез келген үлкен санға тең болуы мүмкін.

Осы арқылы ең басты қорытындыға келеміз: егер қосу және көбейту амалдарын өзара салыстыратын болсақ, онда көбейту амалы бірнеше немесе көптеген қосу амалынан тұратын болғандықтан қосу амалына қарағанда анағұрлым күрделірек болады.

Бұл жәй бақылау компьютер әлемінде үлкен қорытындыға алып келеді, онда орындалатын арифметикалық амалдар қиындығына қарай оңай – қосу амалы, аса күрделі – көбейту амалы деген ережеге негізделеді.

14. Көбейту кестесін не үшін «жаттау» керек? Күнделікті өмірде еш себепсіз жаттап алу керек дүниелер жетерлікті, мысалы жақындардың аттары мен туған күндері, тұрғылықты жерлері мен телефондары, заман табалына сай ЖСН (жеке сәйкестендіру нөмірі) нөмірлері және т.с.с.

Математикадағы көбейту амалы да қосу амалы сияқты өмірде жиі қолданылады, мәселен, дүкенге барған сәттің өзінде бір заттан бірнеше дана алу кезінде оның бағасын осы көбейту амалы арқылы есептеуге тура келеді. Әрине, бұл амалдың мағынасын және қалай орындалатындығын түсініп алғаннан кейін осындай қажетті сәттерде «таяқша» әдісін қолданып тұру тиімсіз әрі мүмкін емес. Сондықтан, көбейту амалының мағынасын түсінгеннен кейін көбейту кестесін жаттап алған жөн, ол кез келген орынды сандарды бағанмен көбейтуге мүмкіндік береді.

Мәселен, 17 және 21 сандары үшін қосу және көбейту амалдарын орындайық.

$$\begin{array}{r} 17 \\ +\ 21 \\ \hline 38 \end{array} \text{ және } \begin{array}{r} 17 \\ \times\ 21 \\ \hline +\ 17I4 \\ \hline 357 \end{array}$$

Сонымен, ол ең жоқ дегенде көбейту амалын «баған» арқылы қолмен санау кезінде, бірдей қосылғыштарды есептеген сайын уақыт шығындамай жылдам орындау үшін қажет.

15. Көбейту амалының орынауыстырымдық қасиеті. Қосу амалындағы алынған сандардың ретінің маңызды еместігін білдіретін ауыстырымдылық қасиеті көбейту амалы үшін де орындалады, яғни мектеп математикасындағы жатталатын екінші тақпақ-ереже «Көбейткіштердің орны ауысқанымен көбейтінді мәні өзгермеуі». Бірақ бұнда да, қосудағыдай балаға «таяқшалар» деңгейінде түсіндіру маңызды, қарапайым $3 \times 4 = 4 \times 3$ теңдігін қарастырайық. Алдымен, енгізілген 3×4 амалының анықтамасының затына «таяқшалар» тілімен көшіп:

$$3 \times 4 = 4 + 4 + 4 = \underset{1\,2\,3\,4}{||||} + \underset{1\,2\,3\,4}{||||} + \underset{1\,2\,3\,4}{||||} = \underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{||||||||||||} = 12,$$

12 таяқшаны біріктіріп алғаннан кейін оқушыға оларды басқаша үш-үштен топтастыру ұсынылады (әрине бұны алдымен шынайы таяқшалардың көмегімен жүргізіп алып,

артынша дәптерге сызу арқылы жасау тиімді):

$$\underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|} = \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|}.$$

Енді көбейту амалы анықтамасының «затынан атына көшу» форматында бұл 4×3 болатындығына көз жеткізгеннен кейін, барлығын қосып санап, оның да мәні 12 санына тең екендігіне көз жеткізу арқылы қайсысы қай орында (бірінші ма, екінші ма) бәрі-бір екендігін аламыз:

$$4 \times 3 = \begin{array}{ccc|ccc|ccc|ccc} | & | & | & | & | & | & | & | & | & | & | & | \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{array} = \underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|} = 12.$$

Дәл осы қасиетті басқа (Шапен Ажғалиев ұсынған) әдіспен де дәлелдеуге болады. Оны «Кірпіштер әдісі» деп атайық және оны мұғалім де, ата-ата да арнайы сынып ішінде отырып қана емес, серуендеу кезінде де кез келген кірпіш үйдің қабырғасын жанынан бір, қырынан бір қаратып, одан кейін оларды үш-үштен топтап алып, бір жағынан санаса да, төрт-төрттен топтастырып екінші жағынан санаса да бәрі-бір сол 12 шығатындығын көрсетуге болады.

Кейін оны дәптермен бекіту баланың сенімділігін арттырады. Ол үшін төрт бағаннан және үш жолдан тұратын кесте сызып, олардың әрқайсысына 1 цифрін жаздыру қажет:

1	1	1	1	4
1	1	1	1	4
1	1	1	1	4

Бұндағы бірліктерді санатсақ, бала 12 шығатындығын көреді. Енді осы санақты әр жол бойынша жеке жүргізуді тапсырсақ, әр жолда 4 бірліктен бар және олар 3 жолда орналасқан, онда көбейтудің оқылуы «3 жолдағы төрт бірлік» түрінде оқылып, «затынан атына » форматында 3×4 көбейтіндісіне келеміз:

$$4 + 4 + 4 = \underset{1\,2\,3\,4}{|\,|\,|\,|} + \underset{1\,2\,3\,4}{|\,|\,|\,|} + \underset{1\,2\,3\,4}{|\,|\,|\,|} = \underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|} = 12$$

және

$$4 + 4 + 4 = 3 \times 4 = 12.$$

Енді, керісінше, бағанмен қосындыласақ, әр бағанда үш бірліктен 4 баған бар, яғни 3 бірліктен 4 баған, бұл 4×3 амалының дәл өзі:

1	1	1	1
1	1	1	1
1	1	1	1
3	3	3	3

$$3 + 3 + 3 + 3 = 4 \times 3$$

және

$$\underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|} + \underset{1\,2\,3}{|\,|\,|} = \underset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12}{|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|\,|} = 12\ .$$

16. Жалпы ескертулер. Бұнда Бастауыш мектептің мұғаліміне мақала атындағы тақырыптың «Математикалық кемелдену» жолындағы әдістемесі қандай болуы, баланы оқыту барысында қандай ұстанымдар негізге алынуы керек және олардың қазіргі ғылым аясындағы орындары мүмкіндігіне сәйкес кеңінен айтылған. Ары қарай, бүкіл Мектеп бағдарламасын қамтитын тікелей қолданысқа икемделген әдістемелік жетістіктер [5] басылымда жинақталған.

Әдебиеттер тізімі

1 Темиргалиев Н. Предисловие Главного редактора журнала "Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия Математика. Информатика. Механика" о целях издания и путях их реализации //Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия Математика. Компьютерные науки. Механика. -2018. -Том 122. -№1. - С. 8-69.

2 Темірғалиев Н. Әубакір Б., Баилов Е., Потапов М.К., Шерниязов К. Алгебра және анализ бастамалары,X-XI кластар. –Алматы: Жазушы, 2002. -382 б.

3 Темиргалиев Н., Аубакир Б., Баилов Е., Потапов М.К., Шерниязов К. Алгебра и начала анализа, для X-XIклассов. Алматы: Жазушы, 2002. -423 с.

4 Темиргалиев Н. Математика. Избранное. Методология и методика. Электронное издание. ИТМиНВ ЕНУ имени Л.Н. Гумилева. -2022. -1967 с.

5 Темиргалиев Н. Научный, научно-методический и организационный отчет «Институт теоретической математики и научных вычислений (ИТМиНВ) Евразийского национального университета имени Л.Н.Гумилева в 2019 году (Часть I)» //Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия Математика. Компьютерные науки. Механика. -2020. -Том 130. -№1. -С. 8-58.

G.E. Taugynbayeva [1] , A.Zh. Zhubanysheva [1] , Zh.K. Tabyldiyeva [2] , N. Temirgaliyev [1]

[1] *Institute of Theoretical Mathematics and Scientific Computations of L.N. Gumilyov Eurasian National University, Satpayev str., 2, Nur-Sultan, 010008, Kazakhstan*

[2] *Secondary School No. 46 named after Bauyrzhan Momyshuly, "Zhana orda", 30, Uralsk, Kazakhstan*

METHODS OF TEACHING NUMBERS AND THE OPERATIONS OF ADDITION AND MULTIPLICATION APPLIED TO THEM IN ELEMENTARY SCHOOL AND THE GENERAL PROBLEMS RELATED TO THEM

Abstract. What is the methodology of reaching the level of "mathematical perfection" in primary school, including the number, arithmetic operations used for them, the multiplication table, the displacement law of addition and multiplication operations, what principles should be taken as a basis during the education of the child and their place in the field of modern science is widely stated.

Keywords: Verbal counting, writing down numbers, adding numbers, multiplying numbers, their substitution property, multiplication table.

Г.Е. Тауғынбаева [1] , А.Ж. Жубанышева [1] , Ж.К. Табылдиева [2] , Н.Темиргалиев [1]

[1] *Институт теоретической математики и научных вычислений Евразийского национального университета имени Л.Н. Гумилева, Сатпаева, 2, 010008, Нур-Султан, Казахстан*

[2] *Средняя общеобразовательная школа № 46 имени Бауржана Момышулы, мкр. "Жана орда", 30, Уральск, Казахстан*

МЕТОДИКА ОБУЧЕНИЯ ЧИСЛАМ И ПРИМЕНЯЕМЫМ К НИМ ОПЕРАЦИЯМ СЛОЖЕНИЯ И УМНОЖЕНИЯ В НАЧАЛЬНОЙ ШКОЛЕ И ЛЕЖАЩИЕ В ИХ ОСНОВЕ ОБЩИЕ ПРОБЛЕМЫ

Аннотация. В рамках достижения итоговой "Математической зрелости" на основе современных общих идей искусственного интеллекта предложена методология прямого применения в изложении тем чисел, действий сложения и умножения над ними, самостоятельных постолбцевых вычислений "Таблицы умножения" в Начальной школе.

Ключевые слова: Устный счет, запись чисел, сложение чисел, умножение чисел, переместительный закон чисел, таблица умножения.

References

1 Temirgaliyev N. Introdaction of the Editor-in-Chief of the Journal "The bulletin of the L. N. Gumilyov Eurasian National University. Mathematics. Computer science. Mechanics series" about the issue purposes and the ways of its implementation, The bulletin of the L. N. Gumilyov Eurasian National University. Mathematics. Computer science. Mechanics series. 2018. Vol. 122. №1. P. 8-69.

2 Temirgaliyev N. , Aubakir B. , Bailov Y. , Potapov K. , SHerniyazov K. Algebra zhane analiz bastamalary [Algebra and the beginning of the analysis], X-XI classes, (Zhazushy, Almaty, 2002, 382 p.).

3 Temirgaliyev N. , Aubakir B. , BailovY. , Potapov K. , SHerniyazov K. Algebra zhane analiz bastamalary [Algebra and the beginning of the analysis], X-XI classes, (Zhazushy, Almaty, 2002, 423 p.).

4 Temirgaliyev N. Matematika. Izbrannoe. Metodologiya i metodika. Elektronnoe izdanie[Mathematics. Favorites. Methodology and technique. Electronic edition]. Institut teoreticheskoj matematiki i nauchnyh vychislenij Evrazijskogo nacional'nogo universiteta imeni L.N. Gumileva [Institute of Theoretical Mathematics and Scientific Computations of L.N. Gumilyov Eurasian National University]. 2022. 1967 p.

5 Temirgaliyev N. Scientific, scientific-methodological and organizational report “The Institute of theoretical mathematics and scientific computing (ITMandSC) L.N.Gumilyov Eurasian National University in 2019 year

(Part I)", The bulletin of the L. N. Gumilyov Eurasian National University. Mathematics. Computer science. Mechanics series. 2020. Vol. 130. №1. P. 8-58.

Авторлар туралы мәлімет:

Тауғынбаева Ғлия Ерболовна – ***Байланыс үшін автор***, PhD, Теориялық математика және ғылыми есептеулер институтының аға ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтпаев көш., 2, Астана, 010008, Қазақстан.

Жұбанышева Ақсәуле Жұбанышева –PhD, Теориялық математика және ғылыми есептеулер институтының аға ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтпаев көш., 2, Астана, 010008, Қазақстан.

Табылдиева Жарқынай Қабылқызы– Бауыржан Момышұлы атындағы № 46 орта мектебінің математика пәні мұғалімі, "Жаңа орда" ША, 30, Орал қаласы, Қазақстан.

Темірғалиев Нұрлан – физика-математика ғылымдарының докторы, профессор, Теориялық математика және ғылыми есептеулер институтының директоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтпаев көш., 2, Астана, 010008, Қазақстан.

Taugynbayeva Galiya – ***Corresponding author***, PhD, senior researcher of the Institute of Theoretical Mathematics and Scientific Computations of L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan.

Zhubanysheva Aksaule – PhD, senior researcher of the Institute of Theoretical Mathematics and Scientific Computations of L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan.

Tabyldiyeva Zharkinai – Teacher of mathematics at secondary school No. 46 named after Baurzhan Momyshuly, "Zhana Orda", 30, Ural city, Kazakhstan.

Temirgaliyev Nurlan – doctor of physical and mathematical sciences, director of the Institute of Theoretical Mathematics and Scientific Computations of L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan.

Редакцияға 11.01.2022 қабылданды

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің
хабаршысы. Математика. Компьютерлік ғылымдар. Механика сериясы.
- 2022. 1(138)- Нұр-Сұлтан: ЕҰУ. 55-б.
Шартты б.т. - 4,44.
Ашық қоланыстағы электронды нұсқа: http://bulmathmc.enu.kz/
Авторларға арналған нұсқаулықтар, публикациялық этика журнал сайтында берілген:
http://bulmathmc.enu.kz/

Мазмұнына типография жауап бермейді

Редакция мекен-жайы: 010008, Қазақстан Республикасы, Нұр-Сұлтан қ.,
Сәтпаев көшесі, 2.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Тел.: +7(7172) 70-95-00 (ішкі 31-410)

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің баспасында басылды