

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS

Volume: 02 Issue: 11 | Nov 2021 ISSN: 2660-5309

Исследования Общих Математических Характеристик Моделей Булевых Функций Логических Операций И Табличной Замены В Криптографических Преобразованиях

Д. Е. Акбаров[1], О. Э. Кушматов[2], Ш.А. Умаров[3], А.Н. Фозилов[4]

[1]д.физ.-мат. н., Какандский государственный педагогический институт, Каканд, Узбекистан

[2]к.физ.-мат. н., Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан

[3]исследователь, Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан

[4]доц.к.физ.-мат. н, Ферганский политехнический институт, Фергана, Узбекистан

Аннотатсия:

В статье исследованы общие математические характеристики моделей булевых функций логических операций и табличной замены. Предложено правило моделирования аналитической модели таблицы истинности в виде многочлена Жегалкина. Оно является универсальным и позволяет широкого эффективного приложения в разработке аппаратно-программных и программных криптографических средств защиты информации. Кроме того, общность такого свойства предложенного правила обеспечит широкое эффективное приложение в области автоматизации и управления процессов с цифровыми технологиями и средствами.

ARTICLEINFO

Article history:
Received 30 Sep 2021
Revised form 22 Oct 2021
Accepted 17 Nov 2021

Ключевые слова: математическая модель, логическая операция, табличная замена, таблица истинности, регулярность, нерегулярность, битовые соединения, булева функция, многочлен Жегалкина, строка входных блоков, столбец выходных блоков, тождественная таблица истинности, конкатенация блоки, математическая индукция, автоматизация, цифровая технология

----------***----------

Введение. В настоящее время обмениваемые информации в современной информационно-коммуникационной сети, обрабатываются в соответствии цифровыми кодами и технологическими пакетами, техническими и технологическими средствами. Основные технические и технологические средства цифровой обработки, и использования информации, преимущественно образуются преобразованиями булевых функций. Работы [1,2] посвящены к исследованию особенностей и свойств логических операций. Некоторые особенности и свойства логических операций были обобщены к преобразованиям табличной замены битовых соединений [1-7].

Постановка задачи. В предлагаемой статье исследуются общих математических характеристик моделей булевых функций логических операций и табличной замены в приложениях криптографических и других преобразованиях в виде многочлена Жегалкина.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Решение задачи. Приводится некоторые формализации из первоисточников [8,9]. Рассматривается блок битов $x=(x_1,x_2,...,x_n)$ как элементы пространства $GF(2^n)=\{x=(x_1,x_2,...,x_n)\in X: x_i\in\{0;1\}\}$. Пусть этот блок с некоторой операцией или последовательности ограниченного количества некоторых операций преобразуются на элементы другого пространства

$$GF(2^m)=\{y=(y_1,y_2,...,y_m)\in Y: y_i\in\{0;1\}\}$$

и это выражаются булевыми функциями в следующем виде :

$$Y=f(X): GF(2^n)\to GF(2^m)\ (1)$$

Такое преобразование в векторном виде представляется $f(x)=\{f_1(x), f_2(x),..., f_m(x)\}$ где $x_i, y_i\in GF(2)$, т. е. $x_i, y_i=\{0;1\}$.

Для обеспечения компактной, удобной и эффективной разработки средств техники и технологии цифровой обработки информации моделируются булевы функции преобразования таблицы замены (таблица 1.)

Таблица 1. *Таблица истинности булевых функций*

$x_1\ x_2\ldots\ x_{n-1}\ x_n$	$f_1f_2\ldots f_{m-1}f_m$
0=00 … 00	$S_0=s_1(0)s_2(0)...s_{m-1}(0)s_m(0)$
1=00 … 01	$S_1=s_1(1)s_2(1)...s_{m-1}(1)s_m(1)$
…	**…**
$2^n-2=11\ldots10$	$S_{2^n-2}=s_1(2^n-2)s_2(2^n-2)\ldots s_{m-1}(2^n-2)s_m(2^n-2)$
$2^n-1=11\ldots11$	$S_{2^n-1}=s_1(2^n-1)s_2(2^n-1)\ldots s_{m-1}(2^n-1)s_m(2^n-1)$

Пусть количество входных битов n и выходных битов m равны, т. е. $n=m$, кроме того попарно выполняются условия $S_i\neq S_j, i\neq j$, тогда функция (1) имеет обратную функцию

$$X=f^{-1}(Y): GF(2^m)\to GF(2^n).\ (2)$$

Справедливость этого утверждения следует из свойства взаимной однозначности преобразований [10-17].

В общем виде по логической операции $x*y=z$, где переменные принимают два различных значения «0» и «1», и значения z определяются 4 (четыре) попарно разными состояниями значения переменных x и y .[18-27] Эти высказанные можно представить в виде следующей таблицы, которая называется таблицей истинности:

Таблица 2

x * y	**0**	**1**
0	z_{00}	z_{01}
1	z_{10}	z_{11}

где $z_{ij}\in\{0;1\}, i=0.1;\ j=0,1.$ Здесь, переменные z_{ij} принимают два различные значения «0» и «1». Таблицу истинности еще можно предоставить в следующем виде как **таблицу 1.**, т.е.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Таблица 3

$x\ y$	z
00	z_{00}
01	z_{01}
10	z_{10}
11	z_{11}

где $z_{ij} \in \{0;1\}, i = 0.1;\ j = 0,1.$

В качестве примера рассматривается, часто эффективно используемую в криптографических и других преобразованиях, логическую операцию $\oplus$–XOR с соответствующей таблицей истинности:

Таблица 4

$x\ y$	z
00	**0**
01	**1**
10	**1**
11	**0**

По этой таблице истинности моделируется многочлен Жегалкина аналитически выражающий её. Для этого воспользуется универсальным правилом. В столбце z находится элементы со значениями «1» и по соответствующим строкам входных блоков образуются члены многочлена Жегалкина [28-32]. При этим биту с «1» значением ставиться в соответствие сама переменная x или y, а биту с значением «0» ставиться в соответствие отрицание переменной $\bar{x}$ или $\bar{y}$. Таким образом, модель многочлена Жегалкина соответствующая таблице истинности данного примера выгладить в следующем виде:

$$z = \bar{x}y \oplus x\bar{y}. \quad (3)$$

Пользуясь этим предложенным общим правилом можно моделировать и других логических операций введенных в работе [1-3].

Теорема 1. *Пусть над переменными x и y определена некоторая $*$–логическая операция, т.е. $x * y = z$, где $x, y, z \in \{0,1\}$. Допустим, что в таблице истинности этой логической операции на столбце z не все значения «0» или не все значения «1», т.е. эта операция не тождественно с «0» или «1» значением. Тогда аналитическая модель таблицы истинности в виде многочлена Жегалкина образуется следующим образом: в столбце z находится элементы со значениями «1» и по соответствующим строкам входных блоков образуются члены многочлена Жегалкина по правилу, что биту с «1» значением ставиться в соответствие сама переменная x или y, а биту с значением «0» ставиться в соответствие отрицание переменной $\bar{x}$ или $\bar{y}$.*

Теперь переходиться аналитическому моделированию в виде многочлена Жегалкина преобразования табличной замены по его таблице истинности. В начале рассматривается преобразования табличной замены с двумя битовыми соединениями:

В общем виде. В качестве примера.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Таблица 5

x / y	**00**	**01**	**10**	**11**		**x / y**	**00**	**01**	**10**	**11**
00	z_{00}	z_{01}	z_{02}	z_{03}		**00**	**11**	**10**	**01**	**00**
01	z_{10}	z_{11}	z_{12}	z_{13}		**01**	**10**	**01**	**00**	**11**
10	z_{20}	z_{21}	z_{22}	z_{23}		**10**	**01**	**00**	**11**	**10**
11	z_{30}	z_{31}	z_{32}	z_{33}		**11**	**00**	**11**	**10**	**01**

где $z_{ij} \in \{00;01,10,11\}$, $i = 0,1,2,3;\ j = 0,1,2,3.$

Аналогично как выше, эту таблицу можем перезаписать в следующем виде:

В общем виде. *В качестве примера.*

Таблица 6

x=(x_1, x_2) **y=**(y_1, y_2)	**z**		**x=**(x_1, x_2) **y=**(y_1, y_2)	**z=**(z_1, z_2)
00 00	z_{00}		**00 00**	**11**
00 01	z_{01}		**00 01**	**10**
00 10	z_{02}		**00 10**	**01**
00 11	z_{03}		**00 11**	**00**
01 00	z_{10}		**01 00**	**10**
01 01	z_{11}		**01 01**	**01**
01 10	z_{12}		**01 10**	**00**
01 11	z_{13}		**01 11**	**11**
10 00	z_{20}		**10 00**	**01**
10 01	z_{21}		**10 01**	**00**
10 10	z_{22}		**10 10**	**11**
10 11	z_{23}		**10 11**	**10**
11 00	z_{30}		**11 00**	**00**
11 01	z_{31}		**11 01**	**11**
11 10	z_{32}		**11 10**	**10**
11 11	z_{33}		**11 11**	**01**

Отметим, что входные блоки таблицы истинности образованы четырьмя битами из битовых соединений в двух битах: $x=(x_1, x_2)$ и $y=(y_1, y_2)$. А выходные блоки двумя битами – из битовых соединений в двух битах: $z=(z_1, z_2)$. Элементы столбца входных блоков принимают значения от «0» по «15». А элементы столбца выходных блоков принимают значения от «0» по «3», при этом эти значения повторяются по четыре раза. Поступая как в аналитическом моделировании таблицы истинности логических операций в виде многочлена Жегалкина, по очереди для столбцов z_1 и z_2 соответственно моделируются многочлены Жегалкина:

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

$$z_1 = \bar{x}_1\bar{x}_2\,\overline{y}_1\bar{y}_2 \oplus \bar{x}_1\bar{x}_2\,\bar{y}_1 y_2 \oplus \bar{x}_1 x_2\,\bar{y}_1\bar{y}_2 \oplus \bar{x}_1 x_2 y_1 y_2 \oplus$$

$$\oplus x_1\bar{x}_2 y_1\bar{y}_2 \oplus x_1\bar{x}_2 y_1 y_2 \oplus x_1 x_2\,\bar{y}_1 y_2 \oplus x_1 x_2 y_1\bar{y}_2 \qquad (4)$$

и $$z_2 = \bar{x}_1\bar{x}_2\,\overline{y}_1\bar{y}_2 \oplus \bar{x}_1\bar{x}_2 y_1\bar{y}_2 \oplus \bar{x}_1 x_2\,\bar{y}_1 y_2 \oplus \bar{x}_1 x_2 y_1 y_2 \oplus$$

$$\oplus x_1\bar{x}_2\,\bar{y}_1\bar{y}_2 \oplus x_1\bar{x}_2 y_1\bar{y}_2 \oplus x_1 x_2\,\bar{y}_1 y_2 \oplus x_1 x_2 y_1 y_2 \qquad (6)$$

По формулам (4) и (5) непосредственным вычислением, т.е. последовательно задавая значения входных блоков: $(0000)_2 = 0_{10}$, $(0001)_2 = 1_{10}$, $(0010)_2 = 2_{10}$, …, $(1111)_{10} = 15_{10}$, осуществляя вычисление, получим соответствующие выходные блоки таблицы истинности приведенного примера. Очевидно, что *методом математической индукции можно доказать это правило имеет место и для общего случая, т. е. справедливо в случае* $n-$*входов и* $m-$*выходов, где* $n \geq m$. На пример такие преобразования табличной замены можно предоставить в следующем виде:

Таблица 7. *Таблица истинности преобразования табличной замены*

$x \,/\, y$	y_0	y_1	…	y_i	…	y_{2^m-1}
x_0	z_{00}	z_{01}	…	z_{0i}	…	$z_{0,2^m-1}$
x_1	z_{10}	z_{11}	…	z_{1i}	…	$z_{1,2^m-1}$
…	…	…	…	…	…	…
x_i	z_{i0}	z_{i1}	…	z_{ii}	…	$z_{i,2^m-1}$
…	…	…	…	…	…	…
x_{2^m-1}	$z_{2^m-1,0}$	$z_{2^m-1,1}$	…	$z_{2^m-1,i}$	…	$z_{2^m-1,2^m-1}$

Если длина блока соединения битов $m = 2\,бит$, то количество разных таких блоков равно $2^m = 2^2 = 4$, то есть: 00, 01, 10, 11.

В случае $m = 3\,бит$ и имеется места $2^m = 2^3 = 8$, соответственно: 000, 001, 010, 011, 100, 101, 110, 111.

Аналогичным образом, в случае $m = 4$ и $2^m = 2^4 = 16$, и так далее.

Размер таблицы, выражающий результаты табличной замены $m \times m$, числовые значения $z_{ij} = \left(z_{ij}^0 z_{ij}^1 \ldots z_{ij}^{2^m-1}\right)_2$ удовлетворяют условию $0 \leq z_{ij} = \left(z_{ij}\right)_{10} \leq 2^m - 1$, длина $m-$*бит* результата преобразования z , выполняемые над $m-$*бит*ными блоками x и y , не изменяется. При этом длина входных блоков «xy» преобразования таблицы замены равняется *2m*, а длина выходных блоков «z_{ij}» равняется *m*.

Определение 1. *Если в таблице истинности табличной замены значения* $0 \leq z_{ij} = \left(z_{ij}\right)_{10} \leq 2^m - 1$ *распределены равны (по* 2^m *раза) или неравны, то они соответственно называются преобразованиями табличной замены равномерно распределенными или неравномерно распределенными (регулярными или нерегулярными).*

Аналогично как выше, эту таблицу можем перезаписать в следующем виде:

В общем виде. *В качестве примера.*

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Таблица 8

$\mathbf{x}=(x_1,x_2,...,x_m)$ $\mathbf{y}=(y_1,y_2,...,y_m)$	$z=(z_1,z_2,...,z_m)$		$\mathbf{x}=(x_1,x_2,...,x_m)$ $\mathbf{y}=(y_1,y_2,...,y_m)$	$\mathbf{z}=(z_1,z_2...,z_m)$
00…0 00…0	z_{00}		**00…0 00…0**	**11…111**
00…0 00…1	z_{01}		**00…0 00…1**	**00…010**
00…0 00…10	z_{02}		**00…0 00…10**	**00…001**
00…0 00…11	z_{03}		**00…0 00…11**	**01…000**
… …	**…**		**… …**	**…**
11…1 11…1	$z_{2^m-1,2^m-1}$		**11…1 11…1**	**10…111**

где каждое значение z_{ij} на столбце z повторяются ровно по 2^m раза, т.е. таблица истинности регулярным свойством или не все значения $z_{ij}=const\in\{0,1,...,2^m-1\}$, т.е. это преобразование не тождественное.

Приводиться следующая обобщенная теорема преобразования табличной замены, как в случае преобразования с использованием логических операций.

Теорема 2. *Пусть над переменными* $x=(x_1x_2...x_m)$ *и* $y=(y_1y_2...y_m)$ *определено преобразование табличной замены, т.е.* $xy=(x_1x_2...x_my_1y_2...y_m)=(z_1z_2...z_m)=z$, *где* $x,y,z\in\{0,1,...,2^m-1\}$. *Допустим, что в таблице истинности преобразования табличной замены не все значения* $z_{ij}=const\in\{0,1,...,2^m-1\}$, *т.е. это преобразование не тождественное. Тогда аналитическая модель таблицы истинности в виде многочлена Жегалкина образуется следующим образом: в столбце* z_i, *где* $0\le i\le m$, *выходных блоков* $z=(z_1z_2...z_m)$ *находятся элементы со значениями «1» и по соответствующим строкам входных блоков* $xy=(x_1x_2...x_my_1y_2...y_m)$ *образуются члены многочлена Жегалкина по правилу, что биту с «1» значением ставиться в соответствие сама переменная* x_i *или* y_i, *а биту со значением «0» ставиться в соответствие отрицание переменной* $\bar{x}_i$ *или* $\bar{y}_i$.

По правилу утверждения теоремы аналитическая модель таблицы истинности приведенного примера в виде многочлена Жегалкина выглядеть:

$$z_1=\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...\bar{y}_m\oplus...\oplus x_1x_2...x_my_1y_2...y_m,$$

$$z_2=\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...\bar{y}_m\oplus...\oplus\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...y_{m-1}y_m,$$

$$z_{m-2}=\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...\bar{y}_m\oplus...\oplus x_1x_2...x_my_1y_2...y_m,$$

$$z_{m-1}=\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...\bar{y}_m\oplus\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...y_m\oplus x_1x_2...x_my_1y_2...y_m,$$

$$z_m=\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...\bar{y}_m\oplus\bar{x}_1\bar{x}_2...\bar{x}_m\bar{y}_1\bar{y}_2...y_{m-1}\bar{y}_m\oplus x_1x_2...x_my_1y_2...y_m\ .$$

Теперь коротко отмечается некоторые теоретические и практические научные значимостей.

Анализ полученных результатов. Если обратит внимания на таблицы истинностей преобразования логических операций и табличной замены в качестве входного блока принимается конкатенация

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

блоки $x=(x_1x_2...x_m)$ и $y=(y_1y_2...y_m)$, т.е. $xy=(x_1x_2...x_my_1y_2...y_m)$. А в качестве выходного блока принимается блоки $z=(z_1z_2...z_m)$. Имеют места следующие выводы**:**

1. Если предполагать, что блок $x=(x_1x_2...x_m)$ представляет часть биты открытого сообщения, а блок $y=(y_1y_2...y_m)$ представляет часть биты ключа некоторой длины, кроме того блок $z=(z_1z_2...z_m)$ представляет часть биты шифрованного сообщения, то таблица истинности табличной замены выражает таблицу правило шифрования;
2. Если предполагать, что блоки $x=(x_1x_2...x_m)$ и $y=(y_1y_2...y_m)$ представляют частей биты хешируемого сообщения, а блок $z=(z_1z_2...z_m)$ представляет результат хеширования этих блоков, то таблица истинности табличной замены выражает таблицу правило без ключевого хеширования или сжатия информации;
3. Если предполагать, что блок $x=(x_1x_2...x_m)$ представляет часть биты открытого сообщения передаваемого по сети информационно-коммуникационной сети, а блок $y=(y_1y_2...y_m)$ представляет часть биты исправления ошибок надежной передачи информации, то таблица истинности табличной замены может выражать таблицу кодирования [11, 12] информации.
4. Предложенное правило моделирования аналитической модели таблицы истинности в виде многочлена Жегалкина является универсальным и позволяет широкого эффективного приложения в разработке аппаратно-программных и программных криптографических средств защиты информации.

Отметим, что для преобразования дискретной области определения значения аргумента и изменения значения соответствующими таблицами истинности на основе предложенного правила можно моделировать их аналитическую модель в виде многочлена Жегалкина. Такое свойство обеспечит широкое эффективное приложения предложенного правила в области автоматизации и управления процессов с цифровыми технологиями и средствами.

Заключение. Полученные результаты в компактном математическом виде с соответствующими определениями, утверждениями, их анализами выражают фундаментальные основы. Представляют базовые основы для разработки аппаратно-программных и программных криптографических средств защиты информации с широкими эффективными приложениями.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ

1. Акбаров, Д. Е., & Умаров, Ш. А. (2020). Анализ приложения логических операций к криптографическим преобразованиям средств обеспечения информационной безопасности. *Universum: технические науки*, (2-1 (71)).
2. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. *Scientific-technical journal*, *4*(2), 6-14.
3. Akbarov D. E., Umarov Sh. A. (2020). Applying Logical Operations and table replacements in modeling basic transformations of Symmetric block encryption algorithms. International Journal of Mechanical and Production Engineering Research and Development, Vol. 10, Issue. 3, Jun, 15041-15046. (Scopus)
4. Акбаров, Д. Е., & Умаров, Ш. А. (2020). Алгоритм электронной цифровой подписи на основе композиции вычислительных сложностей: дискретного логарифмирования, разложения на простые множители и сложения точек эллиптической кривой.
5. Умаров, Ш. А., & Акбаров, Д. Е. (2016). Разработка нового алгоритма шифрования данных с

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

симметричным ключом. *Журнал Сибирского федерального университета. Техника и технологии*, *9*(2).

6. Акбаров, Д. Е., Умаров, Ш. А., & Акбаров, Д. Є. (2016). Новый алгоритм блочного шифрования данных с симметричным ключом.
7. Akbarov D. E. (2009). Cryptographic methods of ensuring information security and their application. Tashkent. p. 432.
8. Молдовян, Н. А. (2004). *Криптография: от примитивов к синтезу алгоритмов*. БХВ-Петербург.
9. Молдавян А. А., Молдавян Н. А., (2004). Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. СПб.: БХВ – Петербург, 496 с.
10. Колмогоров, А., & Фомин, С. (2018). *Элементы теории функций и функционального анализа*. Litres.
11. Якимов, А. В., Новиков, Ф. В., & Новиков, Г. В. Физическая сущность и технологические возможности прерывистого шлифования. *И его научная технологическая школа*, *50*, 209.
12. Скляр, Б. (2004). *Цифровая связь: Теоретические основы и практическое применение*. Издательский дом Вильямс.
13. Abdurazakov, A., Makhmudova, N., & Mirzamakhmudova, N. (2021). On one method for solving degenerating parabolic systems by the direct line method with an appendix in the theory of filration.
14. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2020). Численное решение методом прямых интеграла дифференцирования уравнений, связанных с задачами фильтрации газа. *Universum: технические науки*, (7-1 (76)), 32-35.
15. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2019). Решения многоточечной краевой задачи фильтрации газа в многослойных пластах с учетом релаксации. *Universum: технические науки*, (11-1 (68)).
16. Shadimetov, K., & Daliyev, B. (2021, July). Composite optimal formulas for approximate integration of weight integrals. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020025). AIP Publishing LLC.
17. Шадиметов, Х. М., & Далиев, Б. С. (2020). Коэффициенты оптимальных квадратурных формул для приближенного решения общего интегрального уравнения Абеля. *Проблемы вычислительной и прикладной математики*, (2 (26)), 24-31.
18. Sattorov, A. M., & Xujaxonov, Z. Z. (2019). Approach calculation of certain specific integrals by interpolating polynomials. *Scientific Bulletin of Namangan State University*, *1*(3), 10-12.
19. Шаев, А. К., & Нишонов, Ф. М. (2018). Сингулярные интегральные уравнения со сдвигом Карлемана с рациональными коэффициентами. *Молодой ученый*, (39), 7-12.
20. Azizov, M., & Rustamova, S. (2019). The Task of Koshi for ordinary differential equation of first order which refer to equation of Bernoulli. Scientific journal of the Fergana State University, 2(1), 13-16.
21. Хаетов, А. Р., & Расулов, Р. Г. (2020). Расширение квадратурной формулы Эйлера-Маклорена в пространстве W. *Matematika Instituti Byulleteni Bulletin of the Institute of Mathematics Бюллетень Института*, (3), 167-176.
22. Xujaxonov, Z. Z. (2019). Approximate computation by the interpolation polynomial method some curvilinear integrals with singular coefficients. *Scientific Bulletin of Namangan State University*, *1*(6), 22-25.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

23. Abdurazakov, A., Makhmudova, N., & Mirzamakhmudova, N. The numerical solution by the method of direct integrals of differentiation of equations have an application in the gas filtration theorem..
24. Shadimetov, K., & Daliyev, B. (2021, July). Composite optimal formulas for approximate integration of weight integrals. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020025). AIP Publishing LLC.
25. Шадиметов, Х. М., & Далиев, Б. С. (2020). Коэффициенты оптимальных квадратурных формул для приближенного решения общего интегрального уравнения Абеля. *Проблемы вычислительной и прикладной математики*, (2 (26)), 24-31.
26. Hayotov, A. R., Bozarov, B. I., & Abduganiev, A. (2018). Optimal formula for numerical integration on two dimensional sphere. *Uzbek Mathematical Journal*, *3*, 80-89.
27. Bozarov, B. I. (2019). An optimal quadrature formula with sinx weight function in the Sobolev space. *Uzbekistan Academy Of Sciences Vi Romanovskiy Institute Of Mathematics*, 47.
28. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
29. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
30. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
31. Каримов, Ш. Т., & Хожиакбарова, Г. (2017). Аналог задачи гурса для одного неклассического уравнения третьего порядка с сингулярным коэффициентом. *Toshkent shahridagi turin politexnika universiteti*, 121.
32. Tillabayev, B., & Bahodirov, N. (2021). Solving the boundary problem by the method of green's function for the simple differential equation of the second order linear. *ACADEMICIA: An International Multidisciplinary Research Journal*, *11*(6), 301-304.

Copyright (c) 2021 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/