УДК 519.6
Doi: 10.31772/2712-8970-2023-24-4-673-680

Для цитирования: Кузнецов А. А., Кузнецова А. С., Кишкан В. В. Алгоритм быстрого умножения элементов в 2-группах на основе полиномов Жегалкина // Сибирский аэрокосмический журнал. 2023. Т. 24, № 4. С. 673–680. Doi: 10.31772/2712-8970-2023-24-4-673-680.

For citation: Kuznetsov A. A., Kuznetsova A. S., Kishkan V. V. [An algorithm for fast multiplication of elements in 2-groups based on the Zhegalkin polynomials]. *Siberian Aerospace Journal.* 2023, Vol. 24, No. 4, P. 673–680. Doi: 10.31772/2712-8970-2023-24-4-673-680.

Алгоритм быстрого умножения элементов в 2-группах на основе полиномов Жегалкина

А. А. Кузнецов*, А. С. Кузнецова, В. В. Кишкан

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский Рабочий», 31
*E-mail: alex_kuznetsov80@mail.ru

Проектирование сети многопроцессорной вычислительной системы или дата-центра представляет собой важную проблему, в рамках которой осуществляется поиск моделей графов, обладающих привлекательными топологическими свойствами и позволяющих применять эффективные алгоритмы маршрутизации. Указанными свойствами, в частности такими, как высокая симметрия, иерархическая структура, рекурсивная конструкция, высокая связность и отказоустойчивость, обладают графы Кэли. Например, такие базовые топологии сети, как «кольцо», «гиперкуб» и «тор», являются графами Кэли.

Определение графа Кэли подразумевает, что вершины графа являются элементами некоторой алгебраической группы. Выбор группы и ее порождающих элементов позволяет получить граф, отвечающий необходимым требованиям по диаметру, степени вершин, количеству узлов и т. д. Решению данной задачи посвящено большое количество научных статей и монографий.

Для исследования графов Кэли, в первую очередь, необходимо разработать быстрые алгоритмы умножения элементов в данных группах. Такие алгоритмы помогают осуществлять эффективную маршрутизацию на соответствующих графах Кэли.

Цель настоящей работы – создать алгоритм быстрого умножения элементов в конечных 2*-группах, т. е. в группах периода* 2^n.

В первом разделе статьи дано теоретическое обоснование алгоритма. Показано, что элементы данных групп могут быть представлены в виде битовых строк, а их умножение осуществляется на основе полиномов Жегалкина.

Во втором разделе представлен псевдокод алгоритма, на основе которого вычисляются полиномы Жегалкина. На первом этапе алгоритма вычисляется pc-представление группы, на основе которого получают полиномы Холла. На заключительном этапе полиномы Холла преобразуются в полиномы Жегалкина.

В третьем разделе продемонстрирован пример получения полиномов Жегалкина для двупорожденой группы периода 4.

В заключении рассматриваются перспективы применения алгоритма на реальных вычислительных устройствах. Отмечается, что предложенное представление элементов группы в форме битовых векторов позволяет применять их даже на самых примитивных микроконтроллерах.

Ключевые слова: 2*-группа, граф Кэли, полином Жегалкина.*

An algorithm for fast multiplication of elements in 2-groups based on the Zhegalkin polynomials

A. A. Kuznetsov*, A. S. Kuznetsova, V. V. Kishkan

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarskii Rabochii prospekt, Krasnoyarsk, 660037, Russian Federation
*E-mail: alex_kuznetsov80@mail.ru

Network design for a multiprocessor computing system or data center is an important problem where the search for graph models that have attractive topological properties and allow the use of efficient routing algorithms is carried out. Cayley graphs have the indicated properties, in particular such as high symmetry, hierarchical structure, recursive design, high connectivity and fault tolerance.

The definition of the Cayley graph implies that the vertices of the graph are elements of some algebraic group. Selecting a group and its generating elements allows us to obtain a graph that meets the necessary requirements for diameter, degree of vertices, number of nodes, etc. A large number of scientific articles and monographs are devoted to solving this problem.

The goal of this work is to create an algorithm for fast multiplication of elements in finite 2-groups whose exponent is 2^n.

The first section of the article provides a theoretical justification for the algorithm for fast multiplication in finite 2-groups. It is shown that elements of these groups can be represented in the form of bit strings, and their multiplication is carried out based on the Zhegalkin polynomials.

The second section presents the pseudocode of the algorithm on the basis of which the Zhegalkin polynomials are calculated.

The third section demonstrates an example of obtaining the Zhegalkin polynomials for a two-generated group of exponent 4.

In conclusion, the prospects for using the algorithm on the real hardware are discussed.

Keywords: 2-group, the Cayley graph, the Zhegalkin polynomial.

Introduction

Designing a network of a multiprocessor computing system (MCS) or a data center is an important problem in which graph models are searched for that have attractive topological properties and allow the use of effective routing algorithms. Cayley graphs possess these properties, in particular such as high symmetry, hierarchical structure, recursive construction, high connectivity and fault tolerance [1]. For example, such basic network topologies as "ring", "hypercube" and "torus" are Cayley graphs.

The definition of a Cayley graph implies that the vertices of the graph are elements of some algebraic group. The choice of the group and its generating elements allows us to obtain a graph [2] that meets the necessary requirements in diameter, degree of vertices, number of nodes, etc. A large number of scientific articles and monographs have been devoted to solving this problem, among which we highlight the works [3–15].

As it was said, one of the widely used MCS topologies is the k-dimensional hypercube. This graph is given by the k-generated Burnside group of exponent 2. This group has a simple structure and is equal to the direct product of k instances of a cyclic 2-group. A generalization of the hypercube is an n-dimensional torus, which is generated by the direct multiplication of n instances of cyclic subgroups whose orders may not coincide. In articles [16–19], Cayley graphs of Burnside groups of exponents 3, 4, 5 and 7 are studied.

To study Cayley graphs generated by groups of higher exponents, first of all, it is necessary to develop fast algorithms for multiplying elements in these groups. Such algorithms help to implement efficient routing on the corresponding Cayley graphs.

The purpose of this work is to create an algorithm for fast multiplication of elements in finite 2-groups, i.e. in groups of exponent $2n$.

The first section of the article provides a theoretical justification for the algorithm of fast multiplication in finite 2-groups. It is shown that the elements of these groups can be represented as bit strings, and their multiplication is carried out on the basis of Zhegalkin polynomials.

The second section presents the pseudocode of the algorithm on the basis of which the Zhegalkin polynomials are calculated.

In the third section, an example of obtaining Zhegalkin polynomials for a two-generated group of exponent 4 is demonstrated.

In conclusion, the prospects of using the algorithm on real computing devices are considered.

1. Proof of the main result

The theorem. *Let G be an arbitrary finite group* 2*-a group whose order is equal to* 2^n. *Then the following statements will be true:*

1. $\forall x \in G \Rightarrow x = (x_1,..., x_n) \in \mathbb{Z}_2^n$.
2. $\forall x, y, z \in G : x \cdot y = z \Rightarrow z_i = f_i(x, y) \in \mathbb{Z}_2$, *where* $f_i(x, y)$ *are some Zhegalkin polynomials.*

Proof. Any finite 2-group *G* has a pc-presentation (power commutator presentation [3; 4]):

$$G = \{a_1,\dots,a_n \mid a_i^2 = v_{ii}, 1 \le i \le n, [a_k, a_j] = v_{jk}, 1 \le j < k \le n\},$$

where the word v_{jk} at is $1 \le j \le k \le n$ expressed in terms of as $a_{k+1},\dots,a_n$ follows:

$$v_{jk} = a_{k+1}^{x_{k+1}} \dots a_n^{x_n}, x_i \in \mathbb{Z}_2.$$

In this case

$$\forall x \in G \Rightarrow x = a_1^{x_1} \dots a_n^{x_n}, x_i \in \mathbb{Z}_2.$$

Each element of the group *x* is uniquely defined in terms of degrees $x_1,\dots,x_n$, so we can write the elements of the group as follows:

$$\forall x \in G \Rightarrow x = (x_1,..., x_n) \in \mathbb{Z}_2^n.$$

Thus, we can naturally represent the elements of the group in the form of Boolean (bit) vectors of dimension *n*.

Let $x = (x_1,..., x_n)$ and $y = (y_1,..., y_n)$ *be* two arbitrary elements of the group G, consider their multiplication $x \cdot y = z = (z_1,..., z_n)$.

The calculation of degrees is z_i traditionally carried out on the basis of the collective Hall process [3; 4]. However, there is a more efficient way to multiply elements based on Hall polynomials [20]. In this case

$$z_i = x_i + y_i + p_i(x_1,\dots,x_{i-1}, y_1,\dots,y_{i-1}), x_i, y_i, z_i \in \mathbb{Z}_2.$$

Note that the multiplication and addition operations in the field are $\mathbb{Z}_2$ identical to the Boolean operations "and", as well as the exclusive "or", respectively. By performing the specified substitution of operations in Hall polynomials, we obtain Zhegalkin polynomials [21]. Thus,

$$\forall x, y, z \in G : x \cdot y = z \Rightarrow z_i = f_i(x, y) \in \mathbb{Z}_2,$$

where $f_i(x, y)$ are some Zhegalkin polynomials.

2. Algorithm for calculating Zhegalkin polynomials

In this section, we consider an algorithm for calculating Zhegalkin polynomials for a finite 2-group *G.* The input algorithm knows such parameters of the group as the number of generating elements, the order of G and its exponent. Also, the nilpotence level of the group may appear as an input data.

The pseudocode of the algorithm is shown below.

Input: G – *finite group 2-group G*

Output: *Zhegalkin polynomials for group G*

1. $pc = \mathrm{pq}(G)$ – we calculate the pc-presentation of the group using the p-quotient algorithm [3, 4]. Note that this algorithm has already been implemented in computer algebra systems such as GAP and Magma.

2. $H = \mathrm{Hall}(pc)$ – based on the pc-presentation, we calculate the Hall polynomials using the algorithm from [22].

3. $F = \mathrm{Zhegalkin}(H)$ – we obtain Zhegalkin polynomials from Hall polynomials by replacing the multiplication and summing operations in the field with $\mathbb{Z}_2$ identical Boolean operations "and", as well as the exclusive "or", respectively.

3. An example

As an example, consider the maximum two - generated finite $G = \langle a_1, a_2 \rangle$ period group $2^2 = 4$, which is usually denoted by $B(2,4)$ or $B_2(4)$. The order of this group is equal 2^{12}, and for each element of G there is a unique pc-presentation of the form $a_1^{x_1} \dots a_{12}^{x_{12}}$, where $x_i \in \mathbb{Z}_2$, $i = 1,2,\dots,12$. Here a_1 and a_2 *are* the generating elements G, $a_3 \dots, a_{12}$ calculated recursively through a_1 and a_2.

We obtain a GAP pc-presentation of this group in the computer algebra system.

For brevity, trivial commutator relations are not given (for example, such as $[a_4, a_1] = 1$, etc.).

$a_1^2 = a_4$, $a_2^2 = a_5$, $a_3^2 = a_8 a_9 a_{10} a_{11} a_{12}$, $a_4^2 = 1$, $a_5^2 = 1$, $a_6^2 = a_{11}$, $a_7^2 = a_{11} a_{12}$, $a_i^2 = 1$ $(8 \le i \le 12)$, $[a_3, a_1] = a_6$, $[a_3, a_2] = a_7$, $[a_4, a_2] = a_6 a_8 a_9 a_{10} a_{12}$, $[a_4, a_3] = a_8 a_{11}$, $[a_5, a_1] = a_7 a_8 a_9 a_{10}$, $[a_5, a_3] = a_{10} a_{11} a_{12}$, $[a_5, a_4] = a_9 a_{11}$, $[a_6, a_1] = a_8$, $[a_6, a_2] = a_9$, $[a_6, a_3] = a_{11}$, $[a_6, a_4] = a_{11}$, $[a_6, a_5] = a_{11}$, $[a_7, a_1] = a_9 a_{12}$, $[a_7, a_2] = a_{10}$, $[a_7, a_3] = a_{11} a_{12}$, $[a_7, a_4] = a_{11} a_{12}$, $[a_7, a_5] = a_{11} a_{12}$, $[a_8, a_1] = a_{11}$, $[a_8, a_2] = a_{12}$, $[a_9, a_1] = a_{11} a_{12}$, $[a_9, a_2] = a_{11}$, $[a_{10}, a_1] = a_{12}$, $[a_{10}, a_2] = a_{11} a_{12}$.

Calculate the Hall polynomials of group G for generating elements a_1 and a_2 based on the algorithm from [22]:

1) $a_1 \cdot a_1^{y_1} \dots a_{12}^{y_{12}} = a_1^{z_1} \dots a_{12}^{z_{12}}$, where

$z_1 = y_1 + 1$,

$z_2 = y_2$,

$z_3 = y_3$,

$z_4 = y_1 + y_4$,

$z_5 = y_5$,

$z_6 = y_6 + y_1 y_2$,

$z_7 = y_7$,

$z_8 = y_8 + y_1 y_2 + y_1 y_3$,

$z_9 = y_9 + y_1 y_2$,

$z_{10} = y_{10} + y_1 y_2$,

$z_{11} = y_{11} + y_1 y_3 + y_1 y_2 y_3 + y_1 y_2 y_4 + y_1 y_2 y_5 + y_1 y_2 y_6$,

$z_{12} = y_{12} + y_1 y_2$;

2) $a_2 \cdot a_1^{y_1} \ldots a_{12}^{y_{12}} = a_1^{z_1} \ldots a_{12}^{z_{12}}$, where

$z_1 = y_1$,

$z_2 = y_2 + 1$,

$z_3 = y_1 + y_3$,

$z_4 = y_4$,

$z_5 = y_2 + y_5$,

$z_6 = y_6$,

$z_7 = y_7 + y_1 y_2$,

$z_8 = y_8 + y_1 y_3$,

$z_9 = y_9 + y_1 y_3 + y_2 y_4$,

$z_{10} = y_{10} + y_1 y_2 + y_1 y_3 + y_2 y_3$,

$z_{11} = y_{11} + y_1 y_2 + y_1 y_3 + y_2 y_3 + y_2 y_4 + y_1 y_2 y_3 + y_1 y_2 y_4 + y_1 y_2 y_5 + y_1 y_2 y_7$,

$z_{12} = y_{12} + y_1 y_2 + y_1 y_3 + y_2 y_3 + y_1 y_2 y_3 + y_1 y_2 y_4 + y_1 y_2 y_5 + y_1 y_2 y_7$.

Replace the multiplication and summing operations with the Boolean operations "and", as well as the exclusive "or", respectively. As a result, we obtain the Zhegalkin polynomials.

Each element of the group is a bit string $(z_1, z_2, \ldots, z_{12})$. Thus, it will $B(2,4)$ take 12 bits to encode one element in. In general, if the order of the group is equal 2^n, then it will take n bits to store one element.

Conclusion

In conclusion, we say that in tasks requiring the calculation of a large number of multiplications of group elements, the method described in this paper will dramatically reduce the running time of computer programs. For example, one of these problems is the task of finding the shortest routes on Cayley graphs, which are often used in the design of topologies for interprocessor connection networks in supercomputers, as well as data centers.

In addition, it should be noted that the proposed presentation of the group elements in the form of bit vectors allows them to be used even on the most primitive microcontrollers.

Библиографические ссылки

1. Heydemann M. Cayley graphs and interconnection networks, in Graph symmetry: algebraic methods and applications (Editors: Hahnand Sabidussi) // Dordrecht: Kluwer Academic Publishers. 1997. P. 167–226.

2. Loz E. New record graphs in the degree-diameter problem // Australasian Journal of Combinatorics. 2008. Vol. 41. P. 63–80.

3. Sims C. Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.

4. Holt D., Eick B., O'Brien E. Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.

5. Schibell S., Stafford R. Processor interconnection networks and Cayley graphs // Discrete Applied Mathematics. 1992. Vol. 40. P. 337–357.

6. Stamoulis G., Tsitsiklis J. Effcient routing Scheme for Multiple Broadcasts in Hypercubes // IEEE Trans. on Parallel and Distributed Systems. 1993. Vol. 4(7). P. 725–739.

7. Stamoulis G., Tsitsiklis J. The Effciency of Greedy Routing in Hypercubes and Butteries // IEEE Transaction on Communication. 1994. Vol. 42(11). P. 3051–3061.

8. Kiasari A., Sarbazi-Azad H. Analytic performance comparison of hypercubes and star graphs with implementation constraints // Journal of Computer and System Sciences. 2008. No. 6. P. 1000–1012.

9. Akers S., Krishnamurthy B. A group theoretic model for symmetric interconnection networks // Proceedings of the International Conference on Parallel Processing. 1986. P. 216–223.

10. Tang K., Arden B. Vertex-transitivity and routing for Cayley graphs in GCR representations // Proceedings of ACM Symposium on Applied Computing SAC. 1992. P. 1180–1187.

11. Wang L., Tang K. Topology-Based Routing for Xmesh in Wireless Sensor Networks // Lecture Notes in Electrical Engineering. 2009. Vol. 44. P. 229–239.

12. Ryu J., Noel E., Tang K. Fault-tolerant Routing on Borel Cayley Graph // IEEE ICC Next Generation Networking Symposium. 2012. P. 2872–2877.

13. On the feasibility of completely wireless datacenters / J. Shin, E. Sirer, H. Weatherspoon, D. Kirovski // EEE/ACM Transaction On Networking. 2013. Vol. 21(5). P. 1666–1679.

14. Кузнецов А. А., Кузнецова А. С. Параллельный алгоритм для исследования графов Кэли групп подстановок // Вестник СибГАУ. 2014. № 1(53). С. 34–39.

15. Efficient Routing in Data Center with Underlying Cayley Graph / M. Camelo, D. Papadimitriou, L. Fabrega, P. Vila // Proceedings of the 5th Workshop on Complex Networks CompleNet. 2014. P. 189–197.

16. Кузнецов А. А. Графы Кэли бернсайдовых групп периода 3 // Сибирские электронные математические известия. 2015. Т. 12. С. 248–254.

17. Кузнецов А. А., Кузнецова А. С Перспективные топологии многопроцессорных вычислительных систем, основанные на графах Кэли, заданных группами периода 4 // Вестник СибГАУ. 2016. № 3(17). С. 575–578.

18. Кузнецов А. А. Об одном алгоритме вычисления функций роста в конечных двупорожденных группах периода пять // Прикладная дискретная математика. 2016. № 3(33). С. 116–125.

19. Kuznetsov A. A., Kishkan V. V. The Cayley graphs of finite two-generator burnside groups of exponent 7 // Siberian Journal of Science and Technology. 2018. № 2. P. 217–222.

20. Hall P. Nilpotent groups, Notes of lectures given at the Canadian Mathematical Congress 1957 Summer Seminar, in The collected works of Philip Hall. Oxford: Clarendon Press, 1988. P. 415–462.

21. Яблонский С. В. Введение в дискретную математику. М. : Наука, 1986. 384 с.

22. Кузнецов А. А., Кузнецова А. С. Быстрое умножение элементов в конечных двупорожденных группах периода пять // Прикладная дискретная математика. 2013. № 1 (18). С. 110–116.

References

1. Heydemann M. Cayley graphs and interconnection networks, in Graph symmetry: algebraic methods and applications (Editors: Hahnand Sabidussi). *Dordrecht: Kluwer Academic Publishers*. 1997, P. 167–226.

2. Loz E. New record graphs in the degree-diameter problem. *Australasian Journal of Combinatorics*. 2008, Vol. 41, P.63–80.

3. Sims C. Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994, 628 p.

4. Holt D., Eick B., O'Brien E. *Handbook of computational group theory*. Boca Raton: Chapman & Hall/CRC Press, 2005, 514 p.

5. Schibell S., Stafford R. Processor interconnection networks and Cayley graphs. *Discrete Applied Mathematics*. 1992, Vol. 40, P. 337–357.

6. Stamoulis G., Tsitsiklis J. Effcient routing Scheme for Multiple Broadcasts in Hypercubes. *IEEE Trans. on Parallel and Distributed Systems.* 1993, Vol. 4(7), P. 725–739.

7. Stamoulis G., Tsitsiklis J. The Effciency of Greedy Routing in Hypercubes and Butteries. *IEEE Transaction on Communication*. 1994, Vol. 42(11), P. 3051–3061.

8. Kiasari A., Sarbazi-Azad H. Analytic performance comparison of hypercubes and star graphs with implementation constraints. *Journal of Computer and System Sciences*. 2008, No. 6, P. 1000–1012.

9. Akers S., Krishnamurthy B. A group theoretic model for symmetric interconnection networks. *Proceedings of the International Conference on Parallel Processing*. 1986, P. 216–223.

10. Tang K., Arden B. Vertex-transitivity and routing for Cayley graphs in GCR representations. *Proceedings of ACM Symposium on Applied Computing SAC*. 1992, P. 1180–1187.

11. Wang L., Tang K. Topology-Based Routing for Xmesh in Wireless Sensor Networks. *Lecture Notes in Electrical Engineering*. 2009. Vol.44. P. 229–239.

12. Ryu J., Noel E., and Tang K. Fault-tolerant Routing on Borel Cayley Graph // *IEEE ICC Next Generation Networking Symposium*. 2012, P. 2872–2877.

13. Shin J., Sirer E., Weatherspoon H., Kirovski D. On the feasibility of completely wireless datacenters. *EEE/ACM Transaction On Networking*. 2013, Vol. 21(5), P. 1666–1679.

14. Kuznetsov A. A., Kuznetsova A. S. [A parallel algorithm for study of the Cayley graphs of permutation groups]. *Vestnik SibGAU*. 2014, No. 1(53), P. 34–39 (In Russ.).

15. Camelo M., Papadimitriou D., Fabrega L., Vila P. Efficient Routing in Data Center with Underlying Cayley Graph. *Proceedings of the 5th Workshop on Complex Networks CompleNet*. 2014. P. 189–197.

16. Kuznetsov A. A. [The Cayley graphs of Burnside groups of exponent 3]. *Siberian Electronic Mathematical Reports*. 2015, Vol. 12, P. 248–254 (In Russ.).

17. Kuznetsov A. A., Kuznetsova A. S. [Perspective topologies of multiprocessor computing systems based on the Cayley graphs of groups of period 4]. *Vestnik SibGAU*. 2016, No. 3 (17), P. 575–578 (In Russ.).

18. Kuznetsov A. A. [An algorithm of computation of the growth functions in finite two-generated groups of exponent five]. *Prikladnaya Diskretnaya Matematika*. 2016, No. 3 (33), P. 116–125 (In Russ.).

19. Kuznetsov A. A., Kishkan V. V. The Cayley graphs of finite two-generator burnside groups of exponent 7. *Siberian Journal of Science and Technology*. 2018. No. 2, P. 217–222 (In Russ.).

20. Hall P. Nilpotent groups, Notes of lectures given at the Canadian Mathematical Congress 1957 Summer Seminar, in The collected works of Philip Hall. Oxford: Clarendon Press, 1988. P. 415–462.

21. Yablonsky S. V. *Vvedeniye v diskretnuyu matematiku* [Introduction to discrete mathematics]. Moscow, Nauka Publ., 1989, 384 p.

22. Kuznetsov A. A., Kuznetsova A. S. [Fast multiplication in finite two-generated groups of exponent five]. *Prikladnaya Diskretnaya Matematika*. 2013, No. 1 (18), P. 110–1116 (In Russ.).

Кузнецов Александр Алексеевич – доктор физико-математических наук, профессор, директор НОЦ «Институт космических исследований и высоких технологий»; Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: alex_kuznetsov80@mail.ru.

Кузнецова Александра Сергеевна – кандидат физико-математических наук, доцент кафедры прикладной математики; Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: alexakuznetsova85@gmail.com.

Кишкан Владимир Владимирович – кандидат физико-математических наук, доцент кафедры информатики и вычислительной техники; Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: kishkan@mail.ru.

Kuznetsov Alexander Alexeevich – Dr. Sc., Professor, Head of Institute of Space Research and High Technologies; Reshetnev Siberian State University of Science and Technology. E-mail: alex_kuznetsov80@mail.ru.

Kuznetsova Alexandra Sergeevna – Cand. Sc., Associate Professor of the Department of Applied Mathematics; Reshetnev Siberian State University of Science and Technology. E-mail: alexakuznetsova85@gmail.com.

Kishkan Vladimir Vladimirovich – Cand. Sc., Associate Professor of the Department of Informatics and Computer Science; Reshetnev Siberian State University of Science and Technology. E-mail: kishkan@mail.ru.