UDC 004.047

[0000-0002-6154-8411] **A. A. Sysoienko,** *Ph. D. Student,*
e-mail: Ampere859@gmail.com
[0000-0002-0009-337X] **S. V. Sysoienko,** *Ph. D., Associate Professor*
e-mail: s.sysoienko@chdtu.edu.ua
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

METHOD FOR MINIMIZATION OF BOOLEAN FUNCTIONS WITH A LARGE NUMBER OF VARIABLES BASED ON DIRECTED ENUMERATION

The development of computer technology directly depends on the development of methods for synthesizing components of digital computer technology, therefore the automation of the process is observed in the development of microcircuits. Boolean algebra is widely used for the synthesis of circuit models, and one of the problems in this case is the dependence of the complexity of implementing a given circuit on the number of variables of the Boolean function that implements it. Based on this, it can be argued that the increase in the number of variables in the functions that require minimization requires the search for new or improvement of existing methods of minimization of Boolean functions, which will be easy to use, descriptive and have the ability to automate the implementation of the minimization process.

The task of developing effective methods of minimization of Boolean functions for simulation of circuits with linear and polynomial dependence of simulation speed on the number of variables of the implemented Boolean function remains relevant.

The object of research is the process of minimization of Boolean functions, which are used in the construction of circuits of digital automata.

The purpose of this work is practical implementation of the method of minimization of Boolean functions based on directed enumeration when increasing the number of variables.

The objective considered in this work is to develop and implement the method of minimization of Boolean functions, which will help to minimize Boolean functions based on directed enumeration, the bitness of which exceeds ten variables, as well as to increase the efficiency of search when bonding implicants with a large uncertainty in the sets of functions. Since all existing methods of minimization face the problem of cumbersome calculations when the number of variables increases, the method of directed enumeration, which is quite effective in the case of large uncertainty in the sets, has been chosen for the study. Based on the calculations, it has been determined that this method of minimization of Boolean functions is efficient and easy to use. Its main advantage is the possibility of implementation by means of computer technology, and directed enumeration as the basis can reduce the requirements for hardware and software resources of automated design systems.

Keywords: *method of minimization, Boolean functions, set of function values, directed enumeration.*

Introduction. The use of algorithms that operate on Boolean structures is typical for solving many applied problems, for example, the study of the operation of circuits consisting of functional elements that can be used to describe the mathematical model of the operation of any computer, minimization of disjunctive normal forms, the problem about the feasibility of the Boolean function, the problem about the absence of tautologies, the problem about the completeness of the set of connections and many others [1]. The rapid development of computer technology has led to the fact that most calculations related to various spheres of human activities are carried out automatically with the help of modern computers. Since the development of computer technology directly depends on the development of methods for synthesizing components of digital computer technology, the automation of the process is also observed in the development of microcircuits. The main work in the development and debugging is allocated to work with the cir-

DOI: 10.24025/2306-4412.1.2023.274914

cuit model, and only after that physical synthesis takes place. Boolean algebra is used for the synthesis of circuit models, that is, circuits are described using analytical expressions of logical functions. One of the problems that arise during the synthesis of circuits is the dependence of the volume (complexity of implementation) of the circuit on the number of variables of the Boolean function that implements it.

One logical function can be described by a set of equivalent representations in the form of logical formulas. It is known that any logical formula can be transformed into a disjunctive normal form (DNF). For this, for example, one needs to use the law of double negation, de Morgan's law, and the law of distributivity.

The disadvantage of the methods for obtaining the functions of a perfect DNF (or a perfect KNF) can be considered that when ensuring, in general, the correct functioning of the devices, the resulting circuits are often unreasonably complex. They require a large number of logical elements and have low efficiency. It is clear that the simpler is the analytical expression of the function, the more economical and simpler is its practical implementation on integrated microcircuits. That is why, when describing, it is necessary to obtain such a version of the formula, so that the logical function has the simplest representation of the logical function. After all, the compactness of the circuit directly depends on the simplicity of the formula of the logical function, and only in this case it is possible to obtain it with the best indicators of implementation complexity. In most cases, it is possible to simplify the logical expression without changing the function. The methods for simplifying a function are called the methods of minimizing functions.

Minimization means the transition from a perfect DNF to a DNF with a minimum of components, while the number of multipliers in each component should also be minimal, that is, it’s necessary to reduce the number of variables and operations in the DDNF as much as possible.

There are quite a lot of minimization methods today, both analytical and graphical ones: the method of direct transformations of logical functions, the method of undefined coefficients, the Quine method, the Quine-McCluskey method, the graphical method, Karnaugh maps, Veitch maps [2]. All of them have advantages and disadvantages, especially depending on the possibility of automating the process of their implementation and the number of variables in the functions to be minimized. At the same time, none of them is universal.

Therefore, the problem of minimization of the Boolean function is the most important stage of the logical synthesis of discrete devices. In the general formulation, the problem of minimization of Boolean functions has not yet been solved, but it is quite well researched in the class of disjunctive-conjunctive normal forms.

Based on this, it can be argued that the increase in the number of variables in the functions that require minimization requires the search for new or improvement of existing methods of minimization of Boolean functions, which will be easy to use, descriptive and have the ability to automate the implementation of the minimization process.

Analysis of recent research sources. Quite a lot of modern research is devoted to the search for new and improvement of existing methods of minimization of Boolean functions, because this problem is relevant even today when synthesizing the models of digital devices to achieve the minimum complexity of their construction. In particular, one of the ways to implement new effective methods of minimization of Boolean functions is their representation in new forms. For example, in [3, 4] it is proposed to implement logical functions in an orthogonal form, which is considered as a promising direction for the development of Boolean algebra, and in [5, 6] the possibility of applying integer mathematical programming to minimization of Boolean functions is considered. When considering Boolean functions, typical of circuits that implement arithmetic operations, the gain is even greater. In addition, AND/EXOR circuits are easier to diagnose [7, 8]. The proposed method of minimization of 5-bit Boolean functions has a number of features for solving the problem of minimization of the logical function [8].

In [10], a description of a new method for minimizing Boolean functions in an orthogonal form of representation and obtaining a minimal DNF by step-by-step parallel decomposition of Boolean functions into an orthogonal form of representation is given during the allocation of

DOI: 10.24025/2306-4412.1.2023.274914

argument numbers to the basic and informational parts, respectively. It is shown that the proposed method of minimization of Boolean functions in an orthogonal form isn't inferior to the generally accepted methods of minimization by the implementation complexity factor and has the advantage that there is no need to perform additional minimization of intermediate results.

In addition, methods such as minimization by parts [11] and parallelization [12, 13] are widely used for minimization of Boolean functions, especially with a large number of variables.

To date, all possibilities for increasing the stability of cryptographic systems based on the use of logical operations (Boolean functions) of cryptographic transformation have not been exhausted. Cryptotransformation operations built on the basis of logical functions deserve special attention [14-15].

Although powerful studies have been conducted and promising results have been obtained regarding the methods of implementation of Boolean functions, the task of developing effective methods of minimizing Boolean functions for simulation of circuits with linear and polynomial dependence of simulation speed on the number of variables of the implemented Boolean function remains relevant.

The purpose and objectives of the research. The purpose of this work is practical implementation of the method of minimization of Boolean functions based on directed enumeration when increasing the number of variables.

Presenting main material. The method of minimization of functions based on directed enumeration is carried out as follows:

1. The truth table is sorted in ascending order by the values at which the function takes values of zeros and then ones. Thus, the table is divided into two subgroups.

2. The bitness of the truth table is determined and the number of contours of one variable is formed.

3. The presence of combinations of 0 and 1 in the formed contours of the 1st variable is checked.

4. There are three possible cases of distribution of 0 and 1 in the contour:

- the contour contains both zeros and ones;
- there are ones in the contour, but no zeros;
- there are zeros in the contour, but no ones.

5. The contour in which there are no zeros is written into the minimization formula and ones included in it are removed from the list (from the table). Variables and contours are deleted.

6. Recalculation of values in contours with one variable is performed again. If there are ones in the contour, but no zeros, then the search is repeated. If any other option occurs, then it is checked whether there are zeros in the contour, but there are no ones. If there are zeros and no ones, then contours that do not have ones are removed from the list.

7. The next step is to construct contours based on two variables.

8. Contours are built with a bitness equal to the number of variables. Recalculation takes place according to the algorithm described above.

The specificity of this method is that its greatest efficiency is achieved with a large number of undefined values on certain sets of the function.

Example 1. Let's consider the case of minimization of a f_1 Boolean function in four variables with a given option of values (Table 1).

Table 1. **Sorted truth table of the f_1 function**

No.	x_1	x_2	x_3	x_4	f_1
0	0	0	1	0	**0**
1	0	0	1	1	**0**
2	0	1	1	0	**0**
3	1	1	1	0	**0**
4	0	0	0	0	**1**
5	0	0	0	1	**1**
6	0	1	0	1	**1**
7	1	0	0	1	**1**
8	1	0	1	0	**1**
9	1	1	0	0	**1**
10	1	1	0	1	**1**
11	1	1	1	1	**1**

First, let's sort this truth table by the value of the f_1 function in the sets. Next, let's count the number of corresponding contours and enter the obtained values in Table 2.

DOI: 10.24025/2306-4412.1.2023.274914

Table 2. **One-variable contours for the f_1 function**

	0	1	1
1 x_1	1	5	2
2 $\bar{x}_1$	3	3	0
3 x_2	2	4	1
4 $\bar{x}_2$	2	4	1
5 x_3	4	2	2
6 $\bar{x}_3$	**0**	**6**	0
7 x_4	3	5	1
8 $\bar{x}_4$	1	3	1

As a result, we have that the number of zeros in the $\bar{x}_3$ contour is zero, and the number of ones is the maximum. Therefore, the resulting contour is removed from further calculations and is written into the minimal disjunctive normal form (MDNF) of the function.

Let's delete in Table 2 the lines on which the value of the sets coincides with the value of the minimized contour for one $\bar{x}_3$ variable (Table 3).

Table 3. **Deletion of rows in the truth table of the f_1 function**

No.	x_1	x_2	x_3	x_4	f_1
0	0	0	1	0	**0**
1	0	0	1	1	**0**
2	0	1	1	0	**0**
3	1	1	1	0	**0**
4	~~0~~	~~0~~	~~0~~	~~0~~	**1**
5	~~0~~	~~0~~	~~0~~	~~1~~	**1**
6	~~0~~	~~1~~	~~0~~	~~1~~	**1**
7	~~1~~	~~0~~	~~0~~	~~1~~	**1**
8	1	0	1	0	**1**
9	~~1~~	~~1~~	~~0~~	~~0~~	**1**
10	~~1~~	~~1~~	~~0~~	~~1~~	**1**
11	1	1	1	1	**1**

After deletion of lines and recalculating the contours (Table 3), in which the f_1 function takes the value of one, we remove $\bar{x}_1$ from further use, since there are no more ones left in it.

Let's form two-variable contours for the f_1 function (Table 4).

Table 4. **Two-variable contours for the f_1 function**

	0	1	1
1 x_1x_2	1	1	0
2 $x_1\bar{x}_2$	0	1	0
3 x_1x_3	1	2	0
4 x_1x_4	0	1	0
5 $x_1\bar{x}_4$	0	0	0
6 x_2x_3	2	1	0
7 x_2x_4	0	1	0
8 $x_2\bar{x}_4$	2	0	0
9 $\bar{x}_2x_3$	2	1	0
10 $\bar{x}_2x_4$	1	0	0
11 $\bar{x}_2\bar{x}_4$	1	1	0
12 x_3x_4	1	1	0
13 $x_3\bar{x}_4$	3	1	0

Thus, after minimization and recalculation of values, we have that MDNF functions $f_1 = \bar{x}_3 \vee \bar{x}_1x_2 \vee x_1x_4$ or $f_1 = \bar{x}_3 \vee \bar{x}_1x_2 \vee x_2x_4$.

Since the method of minimization of Boolean functions by directed enumeration allows to minimize functions with an arbitrary number of variables, let's consider an example of minimization of six-variable Boolean function (Table 5).

Table 5. **Six-variable truth table for the f_2 function**

No.	x_1	x_2	x_3	x_4	x_5	x_6	f_2
0	0	0	0	0	1	0	0
1	0	0	0	0	1	1	0
2	0	0	0	1	0	1	0
3	0	0	0	1	1	0	0
4	0	0	0	0	0	1	1
5	0	0	1	0	0	1	1
6	0	0	1	0	1	0	1
7	0	0	1	1	0	1	1
8	0	0	1	1	1	0	1

DOI: 10.24025/2306-4412.1.2023.274914

Example 2. Using the values of Table 5, let's form the contours for the one-variable f_2 function (Table 6) and calculate the correspondence between the values of the truth table and one-variable contours for the sets in which the f_2 function takes a zero value and sets in which the function takes a one value.

As a result of the calculations, we have that x_1 and x_2 contours count zero values in the truth table, therefore they are removed from further consideration and do not participate in the formation of two-variable contours, and the x_3 contour is included in the MDNF f_2 function, therefore it also does not participate in the formation of two-variable contours.

The lines covered by the contour are also deleted from the truth table (Table 7).

Table 6. **One-variable contours for the f_2 function**

		0	1	1
1	x_1	**0**	**0**	**0**
2	$\bar{x}_1$	4	5	1
3	x_2	**0**	**0**	**0**
4	$\bar{x}_2$	4	5	1
5	x_3	**0**	**4**	**0**
6	$\bar{x}_3$	4	1	1
7	x_4	**2**	**2**	**0**
8	$\bar{x}_4$	2	3	1
9	x_5	**3**	**2**	**0**
10	$\bar{x}_5$	1	3	1
11	x_6	2	3	1
12	$\bar{x}_6$	**2**	**2**	**0**

Table 7. **Deletion of rows from the truth table of the f_2 function**

No.	x_1	x_2	x_3	x_4	x_5	x_6	f_2
0	0	0	0	0	1	0	0
1	0	0	0	0	1	1	0
2	0	0	0	1	0	1	0
3	0	0	0	1	1	0	0
4	0	0	0	0	0	1	1
5	~~0~~	~~0~~	~~1~~	~~0~~	~~0~~	~~1~~	1
6	~~0~~	~~0~~	~~1~~	~~0~~	~~1~~	~~0~~	1
7	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~	~~1~~	1
8	~~0~~	~~0~~	~~1~~	~~1~~	~~1~~	~~0~~	1

After deletion of rows and columns in the truth table, we recalculate the contours where the function has a one value (Table 8).

Table 8. **Truth table of the f_2 function after deletion**

No.	x_1	x_2	x_4	x_5	x_6	f_2
0	0	0	0	1	0	0
1	0	0	0	1	1	0
2	0	0	1	0	1	0
3	0	0	1	1	0	0
4	0	0	0	0	1	1

It is obvious that x_4, x_5 and $\bar{x}_6$ contours do not participate in the formation of two-variable contours, so we form two-variable contours from such one-vatiable ones: $\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3$, $\bar{x}_4$, $\bar{x}_5$, x_6 (Table 9).

Table 9. **Two-variable contours for the f_2 function**

		0	1	1
1	$\bar{x}_1\bar{x}_2$	4	1	0
2	$\bar{x}_1\bar{x}_4$	2	1	0
3	$\bar{x}_1\bar{x}_5$	1	1	0
4	$\bar{x}_1 x_6$	2	1	0
5	$\bar{x}_2\bar{x}_4$	2	1	0
6	$\bar{x}_2\bar{x}_5$	1	1	0
7	$\bar{x}_2 x_6$	2	1	0
8	$\bar{x}_4\bar{x}_5$	**0**	**1**	0
9	$\bar{x}_4 x_6$	1	1	0
10	$\bar{x}_5 x_6$	1	1	0

DOI: 10.24025/2306-4412.1.2023.274914

Research results. The obtained method provides a positive effect due to the processing of the amount of information greater than the length of the key sequence.

The number of transformation functions in the sets is selected taking into account the bitness of command codes and the bitness of the information being converted. At the same time, the sequence of functions in the sets and their number can additionally provide an increase in the confidentiality of the information transcoding process and guarantee the implementation of requirements for high-speed access.

To quantitatively assess the efficiency of access to information based on the implementation of the developed method, it is proposed to measure the time of cryptographic transcoding in the number of operations of cryptographic addition. A standard cryptosystem provides transcoding during the time of key formation and the time of one cryptographic addition operation. The device provides transcoding in four cryptographic addition operations and the time of key formation.

Calculations of cryptographic transcoding time under the condition of using a four-bit device are presented in Table 10.

Table 10. **Calculations of cryptographic transformation time**

Time of key sequence acquisition	**Cryptographic transcoding time (in the number of cryptographic addition operations)**					
	standard	proposed	standard	proposed	standard	proposed
2	6	8	12	8	24	12
4	10	12	20	12	40	16
6	14	16	28	16	56	20
8	18	20	36	20	72	24
10	22	24	44	24	88	28
12	26	28	52	28	104	32
	2 bits		**4 bits**		**8 bits**	
	Increase of the amount of information					

Since a four-bit cryptographic transformation device is used, we can simultaneously process 2-4 bits of information. When processing 6-8 bits of information, the device will process it in two cycles of operation, 12-16 bits of information – in three cycles of operation, etc.

The results of evaluating the efficiency of cryptographic transformation of information when implementing the developed method under the condition of using a four-bit information transcoding device are shown in Figure 1.

In Figure 1, we have the following designations:

- 0R – standard coding system;
- 1R – system with 2-bit data transformation;
- 2R – system with 4-bit data transformation;
- 4R – system with 8-bit data transformation.

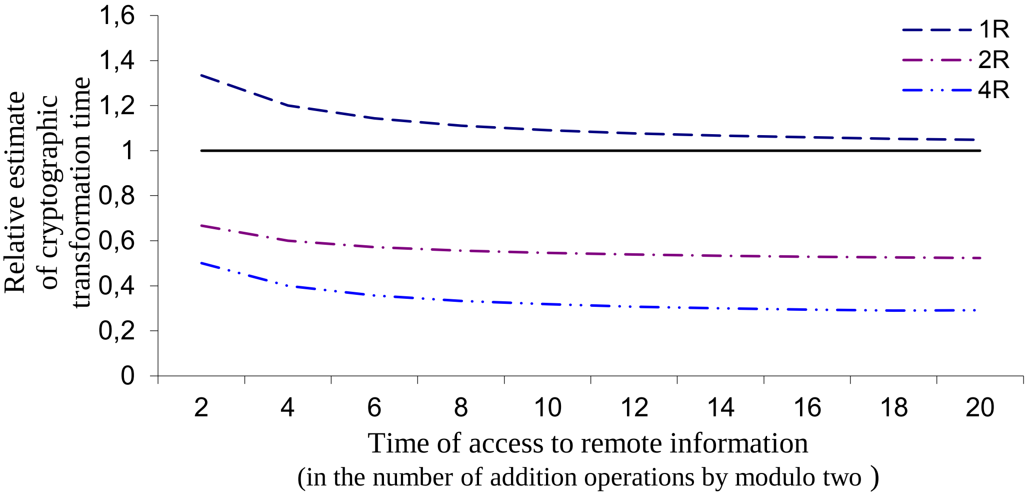

Figure 1. Dependence of the relative estimate of cryptographic transcoding time on the time of access to protected remote information

DOI: 10.24025/2306-4412.1.2023.274914

From the graph shown in Figure 1, it can be seen that the relative estimate of cryptographic transcoding time depends on the amount of processed information and the time of obtaining the key sequence.

Taking into account the calculations of the cryptographic transformation time (Table 10) and the dependence of the relative estimate of cryptographic transcoding time on the time of access to protected remote information (Figure 1), we can confidently conclude that the application of this method allows to increase the speed of access to confidential information from 1.65 up to 3.1 times depending on the key acquisition time and transformation bitness.

Discussion of the result. After counting the contours in this truth table (Table 9), we have found that the $\bar{x}_4\bar{x}_5$ contour at zero value of the function occurs zero times, therefore, it is included in the MDNF of f_2 function.

After deletion of the line covered by the $\bar{x}_4\bar{x}_5$ contour and recalculation of values in the sets in which the function takes the values of one, we have that the $\bar{x}_4\bar{x}_5$ contour has covered all the remaining sets. Therefore, the number of obtained contours is zero, and so the construction of three or more variable contours does not make sense. Consequently, we have obtained MDNF of the $f_2 = x_3 \vee \bar{x}_4\bar{x}_5$ function.

The performed calculations have confirmed the efficiency and simplicity of applying the method of minimization of Boolean functions based on directed enumeration with the number of variables 4 and 6. Moreover, the use of this method of finding MDNF of a function makes it possible to reduce the requirements for software and hardware of automated systems of discrete device design due to the simplicity of implementation of the directed enumeration algorithm, which is the basis of the proposed method.

Conclusions. Therefore, the conducted research on the implementation of the method of minimization of Boolean functions based on directed enumeration makes it possible to affirm that the considered method shows effective results when increasing the number of undefined values in certain sets of functions, which makes it possible to reduce the time of access to confidential information resources from 1.65 to 3.1 times depending on the time of obtaining the key sequence and the transformation bitness.

The implemented method based on directed enumeration has shown the correctness of its use when minimizing Boolean functions with an increased number of variables, and the simplicity of the directed enumeration algorithm allows for its technical implementation on computer equipment. In further scientific research, this method will be used to solve the problem of construction of a discrete model of pseudorandom sequence synthesis using available computing equipment and checking the possibility of increasing the stability of pseudorandom sequences built on the basis of operations of cryptographic transformation to linear cryptanalysis.

References

[1] V. H. Babenko, "A method of increasing the speed of information protection systems based on the use of specialized logical functions", Ph. D. thesis: 05.13.21, Cherkasy, 2009 [in Ukrainian].

[2] IT journal of articles. [Online]. Available: https://www.tutorialspoint.com/automata_theory/dfa_minimization.htm [in Ukrainian].

[3] S. V. Burmistrov, and O. B. Piven, "The matrix method of parallel decomposition as a generalized method of minimization in the orthogonal form of representation", *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, no. 4 (21), pp. 151-157, 2015 [in Ukrainian].

[4] Yu. A. Kochkarev, I. I. Osipenkova, and E. N. Panasko, "Ortogonal forms of presentation of Boolean functions in device blocks", *Visnyk Cherkaskogo derzhavnogo tekhnolohichnogo universytetu*, special issue, pp. 39-42, 2009.

[5] V. F. Senchukov, and T. V. Denysova, "Minimization of Boolean functions by numbers of argument value sets", *Otkrytyie informatsionnyie i kompiuternyie integrirovannyie tekhnologiyi*: sci. papers, Kharkiv: Nats. aerokosm. un-t "KhAI", iss. 83, pp. 156-167, 2019 [in Ukrainian].

[6] V. F. Senchukov, and T. V. Denysova, "v-minimization of Boolean functions by distance matrix and reduction to a mathematical programming problem", *Vidkryti informatsiini ta kompiuterni intehrovani tekhnolohii*: coll. of sci. papers, Kharkiv: Nats. aerokosm. un-t "KhAI", iss. 88, pp. 123-133, 2020 [in Ukrainian]. doi: 10.32620/oikit.2020.88.10.

DOI: 10.24025/2306-4412.1.2023.274914

[7] Kh. Faraj, "Design error detection and correction system based on Reed-Muller matrix for memory protection", *Inter. J. of Computer Applications* (0975-8887), vol. 34, no. 8, pp. 42-55, Nov., 2011. [Online]. Available: https://www.ijcaonline.org/archives/volume34/number8/4123- 5929. doi: 10.5120/4123-5929.

[8] M. T. Solomko, "Minimization of Boolean functions in polynomial and mixed bases by the method of image transformations", in *Twenty-third Int. Sci. and Pract. Seminar Combinatorial Configurations and Their Applications*, Zaporizhzhia-Kropyvnytskyi, May 13-15, 2021, pp. 168-174. [Online]. Available: https://zp.edu.ua/uploads/dept_s&r/2021/conf/1.4/Petrenyuk_ISPS-23-proc.pdf [in Ukrainian].

[9] V. Riznyk, and M. Solomko, "Research of 5-bit Boolean functions minimization protocols by combinatorial method", *Technology Audit and Production Reserves*, vol. 4 (2 (42)), pp. 41-52, 2018. [Online]. Available: https://doi.org/10.15587/2312-8372.2018.140351

[10] Yu. A. Kochkarev, S. V. Burmistrov, and S. F. Aksenov, "Minimization of partially defined Boolean functions in an orthogonal form of representation", *Prikladnaya radioelektronika*, vol. 12, no. 3, pp. 423-430, 2013. [Online]. Available: http://nbuv.gov.ua/UJRN/Prre_2013_12_3_8 [in Russian].

[11] Yu. A. Kochkarev, S. V. Burmistrov, and S. F. Aksenov, "Minimization of Boolean functions by parts", *Radioelektronni i kompiuterni systemy*, no. 4, pp. 110-115, 2012. [Online]. Available: http://nbuv.gov.ua/UJRN/recs_2012_4_18 [in Russian].

[12] S. V. Burmistrov, "Parallel decomposition as the main method of minimizing Boolean functions in an orthogonal form of representation", *Visnyk Cherkaskogo derzhavnogo tekhnolohichnogo universytetu,* no. 2, pp. 67-73, 2014 [in Ukrainian].

[13] S. V. Burmistrov, O. M. Panasco, and N. V. Kovalska, "A matrix method of parallel decomposition for the minimization of symmetric Boolean functions in the form of an extended polynomial", *Visnyk Cherkaskogo derzhavnogo tekhnolohich-nogo universytetu,* no. 1, pp. 130-135, 2018. [Online]. Available: https://doi.org/10.24025/2306-4412.1.2018.162604 [in Ukrainian].

[14] T. V. Myronyuk, S. V. Sysoenko, V. G. Babenko et al., *Information Protection Based on Information-Driven Permutation Operations*: monograph, Cherkasy State Technol. Univ. Cherkasy, Ukraine: publisher Ye. I. Hordienko, 2021, pp. 103-164 [in Ukrainian]. ISBN 978-966-97302-2-0.

[15] S. G. Semenov, and I. V. Myronets, "Improvement of the method of minimization of Boolean functions under the condition of information redundancy", *Systemy upravlinnia, navihatsii ta zviazku*, iss. 3 (35), pp. 92-99, Poltava: PNTU, 2015 [in Ukrainian].

Список використаних джерел

[1] В. Г. Бабенко, "Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій", дис. канд. техн. наук: 05.13.21. Черкаси, 2009.

[2] IT журнал статей. [Електронний ресурс]. Режим доступу: https://www.tutorialspoint.com/automata_theory/dfa_minimization.htm

[3] С. В. Бурмістров, та О. Б. Півень, "Матричний метод паралельної декомпозиції як узагальнений метод мінімізації в ортогональній формі представлення", *Наука і техніка Повітряних Сил Збройних Сил України*: наук.-техн. журн., № 4 (21), с. 151-157, 2015.

[4] Y. A. Kochkarev, I. I. Osipenkova, and E. N. Panasko, "Ortogonal forms of presentation of Boolean functions in device blocks", *Вісник Черкаського державного технологічного університету,* спецвип., с. 39-42, 2009.

[5] В. Ф. Сенчуков, та Т. В. Денисова, "Мінімізація булевих функцій за номерами наборів значень аргументів", *Открытые информационные и компьютерные интегрированные технологии*: науч. тр., Харьков: Нац. аэрокосм. ун-т "ХАИ", вып. 83б с. 156-167, 2019,

[6] В. Ф. Сенчуков, та Т. В. Денисова, "v-мінімізація булевих функцій за матрицею відстаней та зведенням до задачі математичного програмування", *Відкриті інформаційні та комп'ютерні інтегровані технології*: зб. наук. пр., Харків: Нац. аерокосм. ун-т "ХАІ", вип. 88, с. 123-133, 2020. doi: 10.32620/oikit.2020.88.10.

[7] Kh. Faraj, "Design error detection and correction system based on Reed-Muller matrix for

DOI: 10.24025/2306-4412.1.2023.274914

memory protection", *Inter. J. of Computer Applications* (0975-8887), vol. 34, no. 8, pp. 42-55, Nov. 2011. [Online]. Available: https://www.ijcaonline.org/archives/volume34/number8/4123- 5929. doi: 10.5120/4123-5929.

[8] М. Т. Соломко, "Мінімізація булевих функцій у поліномному та змішаному базисах методом образних перетворень", *Двадцять третій Міжнар. наук.-практ. семінар Комбінаторні конфігурації та їх застосування*, Запоріжжя-Кропивницький, 13-15 трав. 2021 р., с. 168-174. [Електронний ресурс]. Режим доступу: https://zp.edu.ua/uploads/dept_s&r/2021/conf/1.4/Petrenyuk_ISPS-23-proc.pdf

[9] V. Riznyk, and M. Solomko, "Research of 5-bit Boolean functions minimization protocols by combinatorial method", *Technology Audit and Production Reserves*, vol. 4(2(42)), pp. 41-52, 2018. [Online]. Available: https://doi.org/10.15587/2312-8372.2018.140351

[10] Ю. А. Кочкарев, С. В. Бурмистров, и С. Ф. Аксенов, "Минимизация частично-определенных булевых функций в ортогональной форме представления", *Прикладная радиоэлектроника*, т. 12, № 3, с. 423-430, 2013. [Электронный ресурс]. Режим доступа: http://nbuv.gov.ua/UJRN/Prre_2013_12_3_8

[11] Ю. А. Кочкарев, С. В. Бурмистров, и С. Ф. Аксенов, "Минимизация булевых функций по частям", *Радіоелектронні і комп'ютерні системи*, № 4, с. 110-115, 2012. [Электронный ресурс]. Режим доступа: http://nbuv.gov.ua/UJRN/recs_2012_4_18

[12] С. В. Бурмістров, "Паралельна декомпозиція як основний метод мінімізації булевих функцій в ортогональній формі представлення", *Вісник Черкаського державного технологічного університету*, № 2, с. 67-73, 2014.

[13] S. V. Burmistrov, O. M. Panasco, & N. V. Kovalska, "Матричний метод паралельної декомпозиції для мінімізації симетричних булевих функцій у вигляді розширеного полінома", *Вісник Черкаського державного технологічного університету*, № 1, с. 130-135, 2018. [Електронний ресурс]. Режим доступу: https://doi.org/10.24025/2306-4412.1.2018.162604

[14] Т. В. Миронюк, С. В. Сисоєнко, В. Г. Бабенко та ін., *Захист інформації на основі операцій перестановок, керованих інформацією*: монографія, Черкас. держ. технол. ун-т. Черкаси, Україна: видавець Гордієнко Є. І., 2021, с. 103-164. ISBN 978-966-97302-2-0.

[15] С. Г. Семенов, та І. В. Миронець, "Вдосконалення методу мінімізації булевих функцій за умови інформаційної надлишковості", *Системи управління, навігації та зв'язку*, вип. 3 (35), с. 92-99, Полтава: ПНТУ, 2015.

А. А. Сисоєнко, *аспірант,*
e-mail: Ampere859@gmail.com
С. В. Сисоєнко, *канд. техн. наук, доцент*
e-mail: s.sysoienko@chdtu.edu.ua
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

МЕТОД МІНІМІЗАЦІЇ БУЛЕВИХ ФУНКЦІЙ З ВЕЛИКОЮ КІЛЬКІСТЮ ЗМІННИХ НА ОСНОВІ НАПРАВЛЕНОГО ПЕРЕБОРУ

Розвиток обчислювальної техніки напряму залежить від розвитку методів синтезу компонентів цифрової обчислювальної техніки, тому автоматизація процесу спостерігається і при розробці мікросхем. Для синтезу моделей схем широко використовується булева алгебра і однією із проблем, що виникають при цьому, вважається залежність складності реалізації певної схеми від кількості змінних булевої функції, що її реалізує.

Виходячи з цього, можна стверджувати, що збільшення кількості змінних у функціях, які потребують мінімізації, вимагає пошуку нових або вдосконалення існуючих методів мінімізації

DOI: 10.24025/2306-4412.1.2023.274914

булевих функцій, що будуть простими у застосуванні, наочними та матимуть можливість автоматизувати реалізацію процесу мінімізації.

Залишається актуальною задача розробки ефективних методів мінімізації булевих функцій для моделювання схем, що мають лінійну та поліноміальну залежність швидкості моделювання від кількості змінних булевої функції, що реалізується.

Об'єкт дослідження – процес мінімізації булевих функцій, які використовуються при побудові схем цифрових автоматів.

Метою роботи є практична реалізація методу мінімізації булевих функцій на основі направленого перебору при збільшенні кількості змінних.

Задача, яка розглядається в цій роботі, полягає в розробці та реалізації методу мінімізації булевих функцій, який дозволить мінімізувати булеві функції на основі направленого перебору, розрядність яких перевищує десять змінних, а також збільшити ефективність пошуку при склеюванні імплікант з великою невизначеністю на наборах функцій.

Оскільки всі існуючі методи мінімізації стикаються з проблемою громіздких обчислень при збільшенні кількості змінних, для дослідження було вибрано саме метод направленого перебору, який є досить ефективним при великій невизначеності на наборах.

На основі проведених розрахунків визначено, що розглянутий метод мінімізації булевих функцій дієвий та простий у застосуванні. Основною його перевагою є можливість реалізації засобами обчислювальної техніки, а покладений в основу направлений перебір дозволяє зменшити вимоги до програмно-апаратних ресурсів систем автоматизованого проектування.

Ключові слова: *метод мінімізації, булеві функції, набір значень функції, направлений перебір.*

Стаття надійшла 02.01.2023
Прийнято 02.02.2023

DOI: 10.24025/2306-4412.1.2023.274914