Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD)
Eurasian Journal of Researches in Social and Economics (EJRSE)
ISSN:2148-9963 www.asead.com

USING COMPLEX CONJUNCTIONS IN SOLVING NONLINEAR BOOLEAN EQUATIONS

Abdussattar Abdukadirovich BAYZHUMANOV[1]
Sh. Sholpan UTEBAEVA[2]
Zagira KOBEYEVA[3]

ABSTRACT

In order to simplify the logical formulations and reduce the time for solving systems of nonlinear Boolean equations, a criterion for the absorption of complex conjunctions by a first-order neighborhood of conjunctions of formulations of a separate class of systems of nonlinear Boolean equations above the second degree, specified by Zhegalkin polynomials, is introduced. In the class of systems of nonlinear Boolean equations under study, the logical formulas of Zhegalkin polynomials are completely or partially divided into some linear factors. As a result, logical formulas are reduced to the disjunction of complex elementary conjunctions, consisting of the product of individual arguments, linear polynomials or their negations, on the basis of which a system of nonlinear Boolean equations is obtained, where the solution to the system of nonlinear equations is obtained using multiplication methods, simultaneously applying the method of reducing complex conjunctions. Some problems of minimization of special disjunctive normal forms obtained from the Zhegalkin polynomial above the second degree of special classes are considered.

Keywords: Zhegalkin polynomial, linear Boolean functions, homogeneous-unit matrices, polynomial length, disjunctive normal forms

[1] Ph.D. ,Associate Professor of the Department of Mathematics, Shymkent University ORCID: 0009-0007-1309-548, absattar52@mail.ru
[2] PhD, the Department of Mathematics, Shymkent University, Utebayeva57@mail.ru
[3] Ph.D. ,Associate Professor of the Department of Mathematics, Shymkent University ORCID:0000-0002-7471-5098 Kobeebazagi82@mail.ru
Araştırma Makalesi/Research Article, Geliş Tarihi/Received: 27/04/2023–Kabul Tarihi/Accepted: 11/05/2023

DOĞRUSAL OLMAYAN BOOLE DENKLEMLERİNİN ÇÖZÜMÜNDE KARMAŞIK BAĞLAÇLARIN KULLANILMASI

ÖZET

Mantıksal formülasyonları basitleştirmek ve doğrusal olmayan Boole denklem sistemlerini çözme süresini azaltmak için, karmaşık bağlaçların, ikincinin üzerindeki ayrı bir doğrusal olmayan Boole denklem sistemleri sınıfının formülasyonlarının birinci dereceden bir komşuluğu tarafından soğurulması için bir kriter Zhegalkin polinomları tarafından belirtilen derece tanıtılır. İncelenmekte olan doğrusal olmayan Boole denklem sistemleri sınıfında, Zhegalkin polinomlarının mantıksal formülleri tamamen veya kısmen bazı doğrusal faktörlere bölünmüştür. Sonuç olarak, mantıksal formüller, sistemin çözümünün bulunduğu, doğrusal olmayan bir Boole denklemleri sisteminin elde edildiği, bireysel argümanların, doğrusal polinomların veya bunların olumsuzlamalarının ürününden oluşan karmaşık temel bağlaçların ayrışmasına indirgenir. doğrusal olmayan denklemlerin sayısı, aynı anda karmaşık bağlaçları azaltma yöntemini uygulayarak çarpma yöntemleri kullanılarak elde edilir. Özel sınıfların ikinci derecesinin üzerinde Zhegalkin polinomundan elde edilen özel ayrık normal formların minimizasyonuna ilişkin bazı problemler ele alınmıştır.

Anahtar Kelimeler: Zhegalkin Polinomu, Doğrusal Boole Fonksiyonları, Homojen Birimli Matrisler, Polinom Uzunluğu, Ayırıcı Normal Formlar

1 INTRODUCTION

The study of logical equations, their classification and the development of effective methods for solving them are of great importance, since it is to them that the solution of many scientific and technical problems that arise, for example, in the synthesis and analysis of discrete computing and control devices, the formalization of the search and proof of theorems, is largely reduced. in formal theories, search for faults in technical systems. These tasks are called logical tasks.

For a long time, a rich source of logical problems has been the theory of automata, using such advanced tools of modern discrete mathematics as graph theory. Automata theory considers complex discrete automatic devices composed of simple elements. Its main problem is the problem of the relationship between the structure and its function, the main task is logical synthesis, the purpose of which is to obtain a structure with predetermined functional properties. The synthesis problem can be formulated as the problem of decomposition of a given function in terms of a system of operators implemented by the elements from which the structure should be built. This task, in turn, is reduced to solving a system of logical equations. The task of analyzing the given structure of a discrete device is also quite important, especially in connection with the problem of troubleshooting. Finding the roots of a system of logical equations is reduced, for example, to the search for stable states of a device, the structure is described by this system [1-5].

Another source of logical problems, which is being intensively developed at the present time, is the problem of creating "artificial intelligence". Within the framework of the problem, a study of tasks is carried out, the formalization of which is associated with great difficulties. Such tasks are usually called "intellectual" or "creative". As a rule, these are also logical problems, many of which can be formulated as problems of solving logical equations of one type or another.

The solution of logical equations in general terms is associated with the need to implement a highly branching process of finding roots, an extensive enumeration of intermediate solutions. As a rule, this is so large that it cannot be realized even by modern high-speed computers. However, taking into account the features of specific equations, the process of finding roots can often be significantly accelerated. Therefore, the main way to develop effective methods for solving logical equations is the classification of equations and the development of appropriate methods for each class.

The paper investigates certain classes of systems of non-linear Boolean equations above the second degree, given by Zhegalkin polynomials. Some problems of minimizing special disjunctive normal forms obtained from the Zhegalkin polynomial above the second degree of special classes are considered. a criterion for the absorption of complex conjunctions by a neighborhood of the first order of conjunctions of propositions of a separate class of systems of non-linear Boolean equations of higher degree two, given by Zhegalkin polynomials, is proposed [6-10].

2 PROBLEM STATEMENT

Here we consider the criteria for analytical takeovers of one complex conjunction by a set of complex conjunctions. Let:

$$\begin{cases} U(\tilde{x},Y(\tilde{x})) = x_{i_1}^{\sigma_1}\cdots x_{i_k}^{\sigma_k} Y_{v_1\cdots v_t}^{\wp_1}\cdots Y_{w_{1\gamma}\cdots w_e}^{\wp}, \\ U_1(\tilde{x},Y(\tilde{x})) = x_{i_1^1}^{\sigma_1^1}\cdots x_{i_{k_1}^1}^{\sigma_{k_1}^1}\cdot Y_{v_1^1\cdots v_{t_1}^1}^{\wp_1^1}\cdots Y_{w_1^1\cdots w_{e_1}^1}^{\wp_{n_1}^1}, \\ \cdots \qquad \cdots \qquad \cdots \\ U_m(\tilde{x},y(\tilde{x})) = x_{i_1^m}^{\sigma_1^m}\cdots x_{i_{k_m}^m}^{\sigma_{k_m}^m}\cdot Y_{v_1^m\cdots v_{t_m}^m}^{\wp_1^m}\cdots Y_{w_1^m\cdots w_{e_m}^m}^{\wp_{n_m}^m}, \end{cases} \tag{1}$$

non-orthogonal complex conjunctions[11] where we denote by $Y_{i_1,\cdots,i_k}$ the sum $x_{i_1}+\cdots+x_{i_k}$: $Y_{i_1,\cdots,i_k}=x_{i_1}+\cdots+x_{i_k}$, here $1\le k\le n; x_{ij}\in X^n=\{x_1,\ldots,x_n\}$, $1\le j\le k$.

Let $M(\tilde{x},\Upsilon(\tilde{x}))=U_1(\tilde{x},\Upsilon(\tilde{x}))\vee\cdots\vee U_m(\tilde{x},\Upsilon(\tilde{x}))$ be a disjunction of compound conjunctions. The problem is formulated as the absorption of a complex conjunction U by a disjunction M etc. $[U\to M]\equiv 1$ or $[U\to \overset{m}{\underset{i=1}{V}} U_i]\equiv 1$[12].

3 CRITERIA FOR ABSORPTION

1–theorem. Disjunction $M(\tilde{x},\mathrm{Y}(\tilde{x}))=U_1(\tilde{x},\mathrm{Y}(\tilde{x}))\vee\cdots\vee U_m(\tilde{x},\mathrm{Y}(\tilde{x}))$ absorbs the complex conjunction $U(\tilde{x},Y(\tilde{x}))$ if and only if

$$\begin{cases} U(\tilde{x},y(\tilde{x}))=1 \\ U_1(\tilde{x},y(\tilde{x}))=0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ U_m(\tilde{x},y(\tilde{x}))=0 \end{cases} \qquad (2)$$

when the system is inconsistent.

Proof. Need. Empty d.n.f. $M(\tilde{x},Y(\tilde{x}))$ absorbs complex conjunction(c.c.)

$$U(\tilde{x},Y(\tilde{x})):\ [U\to M]\equiv 1 \text{ or} [U\to \overset{m}{\underset{i=1}{V}} U_i]\equiv 1. \qquad (3)$$

From here we have $[\bar{U}\vee \overset{m}{\underset{i=1}{V}} U_i]\equiv 1$ or $[U\wedge\neg(\overset{m}{\underset{i=1}{V}} U_i\ )]\equiv 0$.

Let $[U\wedge(\overline{\overset{m}{\underset{i=1}{V}} U_i)}]\equiv 1$. Then there is $\tilde{\alpha}\in E_n^2$ such that $U(\tilde{\alpha})=1$ and $\neg\ (\overset{m}{\underset{i=1}{V}} U_i\left(\tilde{\alpha}\ \right))=1$ or $U(\tilde{\alpha})=1$ and $\overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha})=0$. Therefore, if the system

$$\begin{cases} U(\tilde{x},y(\tilde{x}))=1 \\ U_1(\tilde{x},y(\tilde{x}))=0 \\ \ldots\ldots\ \ldots\ \ldots\ \ldots\ldots \\ U_m(\tilde{x},y(\tilde{x}))=0 \end{cases} \qquad (4)$$

is consistent, then there is a set $\tilde{\alpha}$ such that $U(\tilde{\alpha})=1$, $\overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha})=0$ and $[U(\tilde{\alpha})\wedge\neg(\overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha}))]\equiv 1$. If system (4) is inconsistent, then there is no $\tilde{\alpha}\in E_n^2$ such that $[U(\tilde{\alpha})\wedge\neg(\overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha}))]\neq 1$, etc. $[U(\tilde{\alpha})\wedge\neg(\ \overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha}_i)\ )]=0$ or $[U(\tilde{\alpha})\to \overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha}_i)]=1$. Therefore, when (3) is satisfied, system (2) is inconsistent. **The need has been proven.**

Sufficiency. Let the condition of the theorem be satisfied. Let us show that $[U(\tilde{x},Y(\tilde{x}))\to M(\tilde{x},Y(\tilde{x}))]\equiv 1$. It is easy to see that the set $\tilde{\alpha}\in E_n^2$ in which $U(\tilde{\alpha})=0$ satisfies the equality $[U(\tilde{\alpha})\to M(\tilde{\alpha})]\equiv 1$.

Let now $U(\tilde{\alpha})=1$. Let us show that $\mathrm{M}(\tilde{\alpha})\equiv 1$ and, consequently, the $[U(\tilde{\alpha})\to M(\tilde{\alpha})]\equiv 1.$ Indeed, if system (2) is inconsistent, then there is an equation such that $U_\kappa(\tilde{\alpha})=1$, hence $\overset{m}{\underset{i=1}{V}} U_i(\tilde{\alpha})=1$. So, for any $\tilde{\alpha}\in E_n^2$ we have $[U(\tilde{\alpha})\to M(\tilde{\alpha})]\equiv 1$.

These theorems have been fully proven.

2-theorem: Let $U_1(\tilde{x},Y(\tilde{x})) = x_{i_1}^{\sigma_1}\cdots x_{i_k}^{\sigma_k}\, Y_{v_1^1\cdots v_{\kappa_1}^1}^{\wp_1}\cdots Y_{v_1^t\cdots v_{k_t}^t}^{\wp_t}\cdots Y_{n_1^1\cdots n_{m_1}^1}^{\wp_{t+q+1}}\cdots Y_{n_1^\tau\cdots n_{m_\tau}^t}^{\wp_{t+q+\tau}}$, $U_2(\tilde{x},Y(\tilde{x})) = x_{j_1}^{\alpha_1}\cdots x_{j_c}^{\alpha_c}\cdot Y_{p_1^1\cdots p_{z_1}^1}^{\alpha_{c+1}}\cdot Y_{p_1^2\cdots p_{z_2}^2}^{\alpha_{c+2}}\cdots\cdot Y_{p_1^e\cdots p_{z_e}^e}^{\alpha_{c+e}}$ Complex conjunctions consisting of non-orthogonal expressions. If a $(x_{i_1}^{\sigma_1}\cdots x_{i_k}^{\sigma_k}\to x_{j_1}^{\alpha_1}\cdots x_{j_c}^{\alpha_c})\equiv 1,$

$$\left.\begin{array}{l}
\sum_{i=1}^{t}\wp_i=\alpha_{c+1},\sum_{i=1}^{t}Y_{v_1^i\cdots v_{k_i}^i}=Y_{p_1^1\cdots p_{z_1}^1}\\
\sum_{i=1}^{q}\wp_{t+i}=\alpha_{c+2},\sum_{i=1}^{q}Y_{w_1^i\cdots w_{e_i}^i}=Y_{p_1^2\cdots p_{z_2}^2}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\sum_{i=1}^{\tau}\wp_{t+q+i}=\alpha_{c+e},\sum_{i=1}^{\tau}\gamma_{n_1^i\cdots n_{m_i}^i}=\gamma_{p_1^e\cdots p_{z_e}^e}
\end{array}\right\} \qquad (5)$$

then $[U_1(\tilde{x},y(\tilde{x}))\to U_2(\tilde{x},y(\tilde{x}))]\equiv 1$, etc. the compound conjunction U_1 is absorbed by the compound conjunction U_2.

Proof. Let

$$\begin{cases}\sum_{i=1}^{t}\sigma_i=\sigma,\\ \sum_{\tau=1}^{t}(x_{i_1^\tau}\oplus\cdots\oplus x_{i_{k_\tau}^\tau})=\sum_{i=1}^{e}x_{j_i}\end{cases} \qquad (6)$$

Let us prove that the linear expression $Y_{j_1\cdots j_e}^{\sigma}$ absorbs the product $U(Y(\tilde{x}))=\underset{\tau=1}{\overset{t}{\Delta}}Y_{i_1^\tau\cdots i_{k_\tau}^\tau}^{\sigma_\tau}$, where $U(Y(\tilde{x}))\neq 0$, etc. Equality

$$\left(\bigwedge_{\tau=1}^{t}Y_{i_1^\tau\cdots i_{k_\tau}^\tau}^{\sigma_\tau}\to Y_{j_1\cdots j_e}^{\sigma}\right)\equiv 1 \qquad (7)$$

is true when conditions (6) hold.By Theorem 1, it is known that for the fulfillment of (7) the system

$$\underset{\tau=1}{\overset{t}{\Delta}}Y_{i_1^\tau\cdots i_{k_\tau}^\tau}^{\sigma_1}=1,\; Y_{j_1\cdots j_e}^{\sigma_t}=0 \qquad (8)$$

must be incompatible. Condition $(\underset{\tau=1}{\overset{t}{\Delta}}Y_{i_1^\tau\cdots i_{k_\tau}^\tau}^{\sigma_1}\equiv 0$ implies that the system $\left\{Y_{i_1^1\cdots i_{k_1}^1}^{\sigma_1}=1,\cdots,Y_{i_1^t\cdots i_{k_t}^t}^{\sigma_t}=1\right\}$ or its equivalent system $\left\{Y_{i_1^1\cdots i_{k_1}^1}=\sigma_1,\cdots,Y_{i_1^t\cdots i_{k_t}^t}^{\sigma_t}=\sigma_t\right\}$ are compatible.

It is easy to see that the equations $Y_{j_1\cdots j_e}^{\sigma}=0$, $Y_{j_1\cdots j_e}=\bar{\sigma}$ are equivalent.

Taking into account the above, we construct

$$\begin{cases} Y_{i_1^1 \ldots i_{k_1}^1} = \sigma_1 \\ \cdots \quad \cdots \\ Y_{i_1^t \ldots i_{k_t}^t} = \sigma_t \\ Y_{j_1 \ldots j_l} = \overline{\sigma} \end{cases} \qquad (9)$$

which is equivalent to system (8).

It is known [12] that the system of linear Boolean equations is inconsistent when, after adding the left and right parts of, respectively, unequal constants are obtained. From here it is obvious that the resulting system is inconsistent when equalities (1,2) are satisfied. Consequently, system (8) is inconsistent and therefore takes place.

$$[\mathop{\Delta}_{\tau=1}^{t} Y_{i_1^\tau \cdots i_{k_\tau}^\tau}^{\sigma_\tau} \to Y_{j_1 \cdots j_e}^{\sigma}] \equiv 1 \qquad (10)$$

Means, based on (6) and (7), conditions (5) can be represented as: $(x_{i_1}^{\sigma_1} \cdots x_{i_k}^{\sigma_k} \to x_{j_1}^{\alpha_1} \cdots x_{j_c}^{\alpha_c}) \equiv 1,$

$$\left.\begin{array}{l} \mathop{\wedge}\limits_{i=1}^{t} y_{v_1^i \cdots v_{k_i}^i}^{\vartheta_i} \to y_{p_1^1 \cdots p_{z_1}^1}^{\sigma} \equiv 1, \\ \mathop{\wedge}\limits_{i=1}^{q} y_{w_1^i \cdots w_{e_i}^i}^{\vartheta_t + i} \to y_{p_1^2 \cdots p_{z_2}^2}^{\sigma} \equiv 1, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \mathop{\wedge}\limits_{i=1}^{\tau} y_{m_1^i \cdots n_{m_i}^i}^{\vartheta_{z+q+i}} \to y_{p_1^e \cdots p_{z_e}^e}^{\alpha_{c+e}} \equiv 1, \end{array}\right\} \qquad (11)$$

Hence, it is obvious that when (11) is satisfied, the following is true: $[(\mathop{\wedge}\limits_{j=1}^{k} x_{i_j}^{\sigma_j}).(\mathop{\wedge}\limits_{i=1}^{t} Y_{v_1^i \cdots v_{k_i}^i}^{\vartheta_i}).(\mathop{\wedge}\limits_{i=1}^{q} Y_{w_1^e \cdots w_{e_i}^i}^{\vartheta_{t+i}}) \cdots (\mathop{\wedge}\limits_{i=1}^{\tau} Y_{n_1^i \cdots n_{m_i}^i}^{\vartheta_{t+q+i}}) \to (\mathop{\wedge}\limits_{i=1}^{c} x_{j_i}^{\alpha_i})(\mathop{\wedge}\limits_{i=1}^{e} Y_{p_1^i \cdots p_{z_i}^i}^{\alpha_{c+i}})] \equiv 1,$ or $U_1(\tilde{x}, Y(\tilde{x})) \to U_2(\tilde{x}, Y(\tilde{x})) \equiv 1$.

The theorem is proved.

Let us consider the main criteria for simplifying the disjunctions of complex conjunctions.Let's put

$$U\left(x, Y\left(x\right)\right) = 0 \qquad \text{(identically zero),}$$

$$U_1\left(x, Y\left(x\right)\right) \vee U_2\left(x, Y\left(x\right)\right) = U_2\left(x, Y\left(x\right)\right) \text{(elemental absorption),} \left[U\left(x, Y\left(x\right)\right) \to \mathop{\vee}\limits_{i=1}^{k} U_i\left(x, Y\left(x\right)\right)\right] = 1 \qquad (12)$$

(generalized absorption).

Let $U\left(x, Y\left(x\right)\right) = x_{i_1}^{\sigma_1} \cdots x_{i_l}^{\sigma_l} Y_{v_1 \cdots v_p}^{\delta_1} \cdots Y_{w_1 \cdots w_r}^{\delta_q}$ and

$$\begin{cases} x_{i_1} = \sigma_1, \ldots, Y_{v_1 \ldots v_p} = \delta_1 \\ \quad \cdots \quad \cdots \\ x_{i_l} = \sigma_l, \ldots, Y_{w_1 \ldots w_r} = \delta_q \end{cases} \qquad (13)$$

It is easy to see that system (13) is inconsistent if and only if $x_{i_1}^{\sigma_1}\cdots x_{i_l}^{\sigma_l}Y_{v_1\cdots v_p}^{\delta_1}\cdots Y_{w_1\cdots w_r}^{\delta_q}=0$.

3-theorem. Complex conjunctions

$$Y_{i_1\ldots i_k}^{\sigma_1}\ldots Y_{j_1\ldots j_p}^{\sigma_j}\cdot Y_{\tau_1\ldots\tau_q}^{\sigma_{j+1}},\quad Y_{i_1\ldots i_k}^{\sigma_1}\ldots Y_{j_1\ldots j_p}^{\sigma_j}\cdot Y_{v_1\ldots v_l}^{\sigma} \qquad (14)$$

identically equal if the following conditions are met:

$$\begin{aligned} &a)\ \sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_j\oplus\sigma_{j+1}=\sigma,\\ &b)\ Y_{i_1\ldots i_k}\oplus\ldots\oplus Y_{j_1\ldots j_p}\oplus Y_{\tau_1\ldots\tau_q}=Y_{v_1\ldots v_l}\end{aligned} \qquad (15)$$

Proof.

Condition b) according to the notation of linear expressions can be written as follows: $Y_{v_1\ldots v_l}=Y_{i_1\ldots i_k\ldots j_1\ldots j_p\tau_1\ldots\tau_q}$ therefore, if condition a) is also taken into account, then the complex conjunction (14) has the form : $Y_{i_1\ldots i_k}^{\sigma_1}\ldots Y_{j_1\ldots j_p}^{\sigma_j}\cdot Y_{i_1\ldots i_k\ldots j_1\ldots j_p\ldots\tau_1\ldots\tau_q}^{\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_j\oplus\sigma_{j+1}}$.

Let

$$\begin{aligned}&\left(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_k}\right)^{\sigma_1}=1,\ldots,\left(x_{j_1}\oplus x_{j_2}\oplus\ldots\oplus x_{j_p}\right)^{\sigma_j}=1,\ldots\\ &\left(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_k}\oplus\ldots\oplus x_{j_1}\oplus x_{j_2}\oplus\ldots\oplus x_{j_p}\oplus x_{\tau_1}\oplus x_{\tau_2}\oplus\ldots\oplus x_{\tau_q}\right)^{\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_{j+1}}=\\ &=1\end{aligned} \qquad (16)$$

Hence there is

$$\begin{aligned}&\left(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_k}\right)=\sigma_1,\ldots,\left(x_{j_1}\oplus x_{j_2}\oplus\ldots\oplus x_{j_p}\right)=\sigma_j,\ldots,\\ &\left(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_k}\oplus\ldots\oplus x_{j_1}\oplus x_{j_2}\oplus\ldots\oplus x_{j_p}\oplus x_{\tau_1}\oplus x_{\tau_2}\oplus\ldots\oplus x_{\tau_q}\right)=\\ &=\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_{j+1}\end{aligned} \qquad (17)$$

After simple transformations, we have $x_{\tau_1}\oplus\ldots\oplus x_{\tau_q}=\sigma_{j+1}$ or $Y_{\tau_1\ldots\tau_q}=\sigma_{j+1}$. And this shows that the identity $Y_{i_1\ldots i_k}^{\sigma_1}\ldots Y_{j_1\ldots j_p}^{\sigma_j}\cdot Y_{\tau_1\ldots\tau_q}^{\sigma_{j+1}}$, $Y_{i_1\ldots i_k}^{\sigma_1}\ldots Y_{j_1\ldots j_p}^{\sigma_j}\cdot Y_{v_1\ldots v_l}^{\sigma}$ is true when conditions a) and b) are satisfied. **The theorem has been proven.**

The assertion of the theorem implies the validity of the following corollaries:

Corollary 1. If $\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_l=\overline{\sigma}$ then $x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_1\ldots i_l}^{\sigma}=0$.

Corollary 2. If $\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_l=\sigma$ then $x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_1\ldots i_l}^{\sigma}=x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}$.

Corollary 3. If $\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_l=\sigma$ then $x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_1\ldots i_{l+1}}^{\sigma}=x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot\overline{x_{i_{l+1}}}$.

Corollary 4. If $\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_l=\overline{\sigma}$ then $x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_1\ldots i_{l+1}}^{\sigma}=x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot x_{i_{l+1}}$.

Corollary 5. If $\sigma''=\sigma_1\oplus\sigma_2\oplus\ldots\oplus\sigma_l\oplus\sigma'$ then $x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_1\ldots i_{l+1}\ldots i_k}^{\sigma'}=x_{i_1}^{\sigma_1}\cdot x_{i_2}^{\sigma_2}\cdot\ldots\cdot x_{i_l}^{\sigma_l}\cdot Y_{i_{l+1}\ldots i_k}^{\sigma''}$.

Corollary 6. $Y_{i_1\ldots i_k}^{\sigma_1}\cdot Y_{i_1\ldots i_k i_{k+1}\ldots i_m}^{\sigma_2}=Y_{i_1\ldots i_k}^{\sigma_1}\cdot Y_{i_{k+1}\ldots i_m}^{\sigma_1\oplus\sigma_2}$.

Reduction criterion for systems of nonlinear logical equations of a special class

Let G :

$$\begin{cases} F_1(x_1, x_2, \dots, x_n) = \alpha_1 \\ F_2(x_1, x_2, \dots, x_n) = \alpha_2 \\ \dots \quad \dots \quad \dots \\ F_m(x_1, x_2, \dots, x_n) = \alpha_m \end{cases}$$

system of non-linear Boolean equations.

Moreover, the statement $F(x_1, x_2, \dots, x_n)$ from G has the form:

$$F_1(x_1, x_2, \dots, x_n) = \sum_{i,j=k,i<j}^{k+3} a_{ij} x_i x_j \oplus \sum_{i,j=l,i<j}^{l+3} b_{ij} x_i x_j \oplus$$

$$\sum_{i,j=p,i<j}^{p+3} c_{ij} x_i x_j \oplus \sum_{i,j=q,i<j}^{q+3} d_{ij} x_i x_j \oplus \sum_{i=t}^{t+3} e_i x_i$$

where $k+3 < l, l+3 < p, p+3 < q, q+3 < t$, $\sum_{i,j=k}^{k+3} a_{ij} = \sum_{i,j=l}^{l+3} b_{ij} = \sum_{i,j=p}^{p+3} c_{ij} = \sum_{i,j=q}^{q+3} d_{ij} = 4$

$\{a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_i\} \in \{0,1\}$.

Here the signs $\oplus$, +, $\sum$ – are meant as logical addition on $\bmod 2$.

Here a mum of the form $\sum_{i,j=w}^{w+3} q_{ij} x_i x_j$ and $\sum_{i=v}^{v+3} e_i x_i$ is called the group of elements of the statement F. In addition, the groups of different equations (statements) of the G system do not match in pairs.

The method for solving the system G consists in compact representations of F_i by grouping elements by introducing new variables, transforming the latter into d.n.f. and their simplification. The search for solutions to the system G is carried out using the algorithm for solving the system of linear Boolean equations [1-3].

It is easy to see that the groupings of elements in the statements of the G system are applicable only within individual groups. Obviously, elements of different groups are not grouped.

When grouping elements, there are three cases:

a) each variable is included in exactly two elements of the group;

b) one variable participates in three elements, the other – in one and the remaining two - in two elements;

c) two variables in two elements can also be involved in pairs.

Since the groups in one equation do not intersect in pairs, the grouping and introduction of new variables can be done as follows:

1) $x_i x_j + x_i x_l + x_k x_j + x_l x_j = (x_i + x_j)(x_k + x_l) = Y_{ij} Y_{kl}$;

2) $x_i x_j + x_i x_l + x_k x_i + x_i x_j = x_i(x_j + x_l + x_k) + x_k x_l = x_i Y_{jlk} + x_k x_l$;

3) $x_i x_j + x_i x_l + x_i x_k + x_k x_l = x_i(x_j + x_l) + x_k(x_i + x_l) = x_i Y_{jl} + x_k Y_{il}$;

where $Y_{v_1v_2\ldots v_z} = x_{v_1} + x_{v_2} + \ldots + x_{v_z}$.

Thus, when each variable participates twice in a group, the grouping is done in a unique way. (Case I) . Otherwise, grouping can be done in two ways (case 2 and 3).

The functional of an arbitrary system α , obtained from G by grouping and changing the variable elements of statements, is denoted as follows:

$$\Psi_\alpha = \sum_{y\in\{Y\}} \varphi_y |Y|$$

here $\{Y\}$ is the set of variables in the system α , φ_y is the number of variables in Y , and $|Y|$ is the number of elements in Y .

Example: For $Y_{v_1v_2\ldots v_z} = x_{v_1} + x_{v_2} + \ldots + x_{v_z}$ we have $|Y_{v_1v_2\ldots v_z}| = z$.

The algorithm for grouping system G from a given class is as follows.Groups of elements of statements of the system G are distinguished. All kinds of groupings are made in groups and new variables are introduced. From each group such groupings of elements are selected so that for the resulting system α the functional Ψ_α is the maximum among all functionals Ψ_β of the systems β formed from the groupings of the groups of the system G .

It is easy to see that after grouping and introducing new variables, statements F of system G will contain no more than nine e.c. Note that 17 elementary conjunctions are involved in the initial functions F .It is known [4] that for an arbitrary Zhegalkin polynomial $Q(x_1, x_2, \ldots, x_n) = U_1 + U_2 + \ldots U_t$ where U_i are elementary conjunctions, $i = \overline{1,t}$ we have the equality

$$Q(x_1, x_2, \ldots, x_n) = \bigvee_{\sigma_1+\sigma_2+\ldots+\sigma_t=1} U_1^{\sigma_1} \& U_2^{\sigma_2} \& \ldots \& U_t^{\sigma_t}$$

where $\sigma_j \in \{0,1\}$:

$$U^{\sigma_1} = \begin{cases} U, \text{ if } \sigma = 1 \\ \neg U, \text{ otherwise.} \end{cases}$$

Obviously, from equality , using transformations of analytic expressions, one can obtain a d.n.f. functions Q .

Let the statement F from G after groupings and change of variables have the form:

$$F(z_1, z_2, \ldots, z_l) = \sum_{i=1}^{m} z_i z_i' = \sum_{i=1}^{m} U_i;$$

where $m < 10, l \le 18, z_i, z_i' \in \{x_1, x_2, \ldots, x_n\}, \{Y_{v,w}\}; |v - w| \le 3;$ $v, w = \{1, 2, \ldots, n\}, U_i = z_i z_i';\ z_i z_i' \in \{z_1, z_2, \ldots z_l\}, i = \overline{1,m}.$

Here, logical products will be called complex conjunctions (c.c.).

Now consider the problem of transforming Zhegalkin polynomials consisting of complex conjunctions to complex d.n.f. To do this, we use a more optimal method for Electronic computer

(E.C.) decimal representations of e.c. Consider the decimal representation[5-11] (a_i, b_i) c.c. $U_i \ \left(i=\overline{1,m}\right)$.

It's obvious that $c_i = 0,\ b_i = \sum_{i=1}^{n} \alpha_i 2^{n-i}, \left|\alpha_1, \alpha_2, \ldots, \alpha_l\right| = 2$. Algorithm for converting $F(z_1, z_2, \ldots, z_l)$ to d.n.f. next:

1) C.c. $U_i \left(i=\overline{1,m}\right)$ can be represented as decimal representations of b_i;

2) For each conjunction $U_1^{\sigma_1}, U_2^{\sigma_2}, \ldots, U_m^{\sigma_m}$ in disjunction $F(z_1, z_2, \ldots, z_l) = \underset{\sigma_1+\sigma_2+\ldots+\sigma_t=1}{\vee} U_1^{\sigma_1} \& U_2^{\sigma_2} \& \ldots \& U_t^{\sigma_t}$ where $\sigma_i \in \{0,1\}, i=\overline{1,m}$, we write out all the unit coordinates $\left(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}\right)$ of the set $(\sigma_1, \sigma_2, \ldots, \sigma_m)$. With the help of $b_{i1}, b_{i2}, \ldots, b_{ik}$ we calculate the decimal representation of the conjunction $U_{i1}, U_{i2}, \ldots, U_{ik}$. For the zero coordinates $\sigma_{ij} \left(j=\overline{k+1,m}\right)$ of the set $(\sigma_1, \sigma_2, \ldots, \sigma_m)$ we write out c_{ij}, which are decimal representations of the c.c. $U_{ij} = z_t z_k$. From $b_{ij} = 2^t + 2^k$ we construct $C_1^{ij} = 2^t$ and $C_2^{ij} = 2^k$ corresponding to the c.c. $\neg z_t$ and $\neg z_k$;

3) Using $U_i = \{\neg z_t, \neg z_k\}, i=\overline{1,n-k}$, we construct pairs of all possible s.c. U_{ij} and $\neg z_1, \neg z_2, \ldots, \neg z_{n-k}$, where $\neg z_i \in U_i$ and C_i correspond to c.c. $\neg z_1, \neg z_2, \ldots, \neg z_{n-k}$.

4) For decimal representations (b, c), we write out the corresponding s.c. The result of the algorithm will be d.n.f. feature $F(z_1, z_2, \ldots, z_l)$.

4 SOLUTION OF SYSTEMS OF BOOLEAN NONLINEAR EQUATIONS

Let a system of nonlinear Boolean equations be given, the statements of which consist of disjunctions of complex conjunctions

$$\begin{cases} U_{11} \vee U_{12} \vee \ldots \vee \ldots U_{1,11} = 1 \\ U_{21} \vee U_{22} \vee \ldots \vee \ldots U_{2,12} = 1 \\ \quad \ldots \quad \ldots \quad \ldots \\ U_{m1} \vee U_{m2} \vee \ldots \vee \ldots U_{m,1m} = 1 \end{cases} \tag{18}$$

where $U_{ij} = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \ldots x_{i_k}^{\delta_k} Y_{v_1,w_1}^{\delta_{(k+1)}} \ldots Y_{v_t,w_t}^{\delta_{(k+t)}}$

$$Y^{\delta} = \begin{cases} Y, \ if \ \ \delta = 1, \\ \overline{Y}, \text{otherwise.} \end{cases} \tag{19}$$

It is easy to see that the binary set ά is a solution to system (18) if and only if there exists an equation

$$U_{1,i1} \vee U_{2,i2} \vee \ldots \vee \ldots U_{m,im} = 1 \qquad (20)$$

for which α is the solution.

The algorithm for solving system (18) is as follows: Let $l_j \le l_1, l_2, \ldots, l_{j-1}, l_{j+1}, \ldots, l_m$ or, for simplicity, $l_j = l_1$.

We organize groups for each complex conjunction (c.c.) $U_{1i}\left(i=\overline{1,l_1}\right)$, from system (18), in which: $U_{1i}\left\{U_{k,i1}, U_{k,i2}, \ldots, U_{k,it}\right\} \ne 0$.

$$\begin{cases} U_{1i} = 1 \\ U_{2,i1} \vee U_{2,i2} \vee \cdots \vee U_{2,it_2} = 1 \\ \quad \ldots \quad \ldots \quad \ldots \\ U_{m,i1} \vee U_{m,i2} \vee \cdots \vee U_{m,it_m} = 1 \end{cases} \qquad (21)$$

The multiplication of subsystem equations (21) is carried out by the method of chains, the product of which includes one s.c., which leads to the form (20). Performing operation $U \& U = U$, we represent equation (20) in the following form:

$$x_{j_1}^{\delta_1} x_{j_2}^{\delta_2} \ldots x_{j_k}^{\delta k} Y_{l_1,m_1}^{\delta(l+1)} Y_{l_2,m_2}^{\delta(l+2)} \ldots Y_{l_n,m_n}^{\delta(l+n)} = 1 \qquad (22)$$

With the help of identities:

$$\begin{aligned} & x_i x_j Y_{ij} = 0, \\ & x_i \overline{x_j}\,\overline{Y_{ij}} = 0, \\ & \overline{x_i} x_j Y_{ij} = 0, \qquad (23) \\ & \overline{x_i}\,\overline{x_j} Y_{ij} = 0, \\ & U \& \overline{U} = 0. \end{aligned}$$

we check whether equation (22) has roots.

Next, with the help of transformations:

$$\begin{aligned} & x_i x_j \overline{Y_{ij}} = x_i x_j, && \overline{x_i}\,\overline{Y_{ij}} = \overline{x_i}\,\overline{x_j}, \\ & \overline{x_i} x_j Y_{ij} = \overline{x_i} x_j, && x_i \overline{Y_{ij}} = x_i x_j, \\ & x_i \overline{x_j} Y_{ij} = x_i \overline{x_j}, && x_j Y_{ij} = \overline{x_i} x_j, \\ & \overline{x_i}\,\overline{x_j}\,\overline{Y_{ij}} = \overline{x_i}\,\overline{x_j}, && \overline{x_j} Y_{ij} = x_i \overline{x_j}, \qquad (24) \\ & \overline{x_i} Y_{ij} = \overline{x_i} x_j, && x_j \overline{Y_{ij}} = x_i x_j, \\ & x_i Y_{ij} = x_i \overline{x_j}, && \overline{x_j}\,\overline{Y_{ij}} = \overline{x_i}\,\overline{x_j}. \end{aligned}$$

simplify equation (22).

As a result, we obtain an equation of the form: $x_{t_1}^{\delta_1} x_{t_2}^{\delta_2} \cdots x_{t_k}^{\delta_k} Y_{p_1,q_1}^{\delta(m+1)} Y_{p_2,q_2}^{\delta(m+2)} \cdots Y_{p_t,q_t}^{\delta(m+t)} = 1.$

Bearing in mind that $Y_{ij} = x_i \overline{x_j} \vee \overline{x_i} x_j$, $\overline{Y_{ij}} = \overline{x_i}\,\overline{x_j} \vee x_i x_j$. We build a set of equations of the form $x_{t_1}^{\delta_1} x_{t_2}^{\delta_2} \cdots x_{t_k}^{\delta_k} A_1 A_2 \cdots A_t = 1$, here $A_i, \left(i=\overline{1,t}\right)$ is obtained from $Y_{p_i,q_i}^{\delta_i}$ as follows:

$$A_i \in \left\{ \left(\overline{x_{p_i}}, x_{q_i} \right) \left(x_{p_i}, \overline{x_{q_i}} \right) \right\}, if \;\; \delta_i = 1,$$
$$A_i \in \left\{ \left(x_{p_i}, x_{q_i} \right) \left(\overline{x_{p_i}}, \overline{x_{q_i}} \right) \right\}, if \;\; \delta_i = 0. \qquad (25)$$

Simplifying $x \,\&\, x = x$ and discarding combinations in which the situation $x \,\&\, \neg x = 0$ arises, we obtain a set of equations of the form $x_{i_1}^{\delta_1} \,\&\, x_{i_2}^{\delta_2} \,\&\ldots\&\, x_{i_k}^{\delta_k} = 1$,for each of which we write out the solution $\alpha' = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, where

$$\alpha_\gamma = \begin{cases} \delta_\gamma, \; if \;\; \gamma \in \left(i_1, i_2, \ldots, i_p \right) \\ 2 \end{cases} \qquad (26)$$

5 CONCLUSION

In this paper, separate classes of systems of non-linear Boolean equations above the second degree, given by Zhegalkin polynomials, are investigated. Problems of minimizing special disjunctive normal forms obtained from the Zhegalkin polynomial above the second degree of special classes are solved. A criterion for the absorption of complex conjunctions by a neighborhood of the first order of conjunctions of propositions of a separate class of systems of non-linear Boolean equations of higher degree two, given by Zhegalkin polynomials, is proved.

REFERENCES

[1] Kabulov, A., Baizhumanov, A., Saymanov, I., Berdimurodov, M. "E_ective methods for solving systems of nonlinear equations of the algebra of logic based on disjunctions of complex conjunctions". 2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022, 2022, pp. 95_99

[2] Kabulov, A., Baizhumanov, A., Saymanov, I., Berdimurodov, M. "Algorithms for Minimizing Disjunctions of Complex Conjunctions Based on First-Order Neighborhood Information for Solving Systems of Boolean Equations". 2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022, 2022, pp. 100_104

[3] E. Navruzov and A. Kabulov, "Detection and analysis types of DDoS attack,"2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[4] A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding,"2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

[5] A. Kabulov, I. Normatov, E. Urunbaev and F. Muhammadiev, "Invariant Continuation of Discrete Multi-Valued Functions and Their Implementation,"2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2021, pp. 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422486.

[6] A. Kabulov, I. Normatov, A.Seytov and A.Kudaybergenov, "Optimal Management of Water Resources in Large Main Canals with Cascade Pumping Stations,"2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 2020, pp. 1-4, doi: 10.1109/IEMTRONICS51293.2020.9216402.
[7] Kabulov, A.V., Normatov, I.H. (2019). About problems of decoding and searching for the maximum upper zero of discrete monotone functions. Journal of Physics: Conference Series, 1260(10), 102006. doi:10.1088/1742-6596/1260/10/102006
[8] Kabulov, A.V., Normatov, I.H. Ashurov A.O. (2019). Computational methods of minimization of multiple functions. Journal of Physics: Conference Series, 1260(10), 10200. doi:10.1088/1742-6596/1260/10/102007
[9] Yablonskii S.V. Vvedenie v diskretnuyumatematiku: Ucheb. posobiedlyavuzov. -2e izd., pererab. idop. -M.:Nauka, Glavnayaredaksiya_ziko-matematicheskoy literature, -384 s.
[10] Djukova, E.V., Zhuravlev, Y.I. Monotone Dualization Problem and Its Generalizations: Asymptotic Estimates of the Number of Solutions. Comput. Math. and Math. Phys. 58, 2064_2077 (2018). https://doi.org/10.1134/S0965542518120102
[11] Leont'ev, V.K. Symmetric boolean polynomials. Comput. Math. and Math. Phys. 50, 1447_1458 (2010). https://doi.org/10.1134/S0965542510080142
[12] Nisan, N. and Szegedy, M. (1991). On the Degree of Boolean Functions as Real Polynomials, in preparation.
[13] RamamohanPaturi. 1992. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). In Proceedings of the twenty-fourth annual ACM symposium on Theory of Computing (STOC '92). Association for Computing Machinery, New York, NY, USA, 468_474. https://doi.org/10.1145/129712.129758.
[14] Gu J., Purdom P., Franco J., Wah B.W. Algorithms for the satis_ability (SAT) problem:A Survey // DIMACS Series in Discrete Mathematics and Theoretical Computer Science. 1997.Vol. 35. P. 19_152.
[15] Goldberg E., Novikov Y. BerkMin: A Fast and Robust SAT Solver // Automation andTest in Europe (DATE). 2002. P.142_149.