IRSTI 27.39.25 DOI: https://doi.org/10.26577/JMMCS.2023.v118.i2.02

A.A. Bayzhumanov
South Kazakhstan State Pedagogical University, Kazakhstan, Shymkent
e-mail: absattar52@mail.ru

OPTIMAL METHOD FOR SOLVING SPECIAL CLASSES OF SYSTEMS OF NONLINEAR EQUATIONS OF THE SECOND DEGREE

In order to simplify the notation and reduce the time for solving systems of Boolean equations, a method is proposed that is optimal for solving a separate class of systems of nonlinear Boolean equations of the second degree. In the class of systems of non-linear Boolean equations under study, logical formulas are divided completely or partially into some linear factors. As a result, logical formulas are reduced to a product of linear polynomials, on the basis of which a system of linear Boolean equations is obtained, which is solved an order of magnitude easier than a system of second-order Boolean equations. It is considered some problems of minimization of special disjunctive normal forms obtained from the Zhegalkin polynomial of the second degree of a special class.

Key words: Zhegalkin polynomial, linear Boolean functions, homogeneous-identity matrices, polynomial length, disjunctive normal forms.

А.А. Байжуманов
Оңтүстік Қазақстан мемлекеттік педагогикалық университеті, Қазақстан, Шымкент
e-mail: absattar52@mail.ru

Екінші дәрежелі сызықты емес теңдеулер жүйесінің арнайы кластарын шешудің оңтайлы әдісі

Белгілеулерді жеңілдету және логикалық теңдеулер жүйелерін шешу уақытын қысқарту мақсатында екінші дәрежелі сызықты емес логикалық теңдеулер жүйесінің арнайы класын шешу үшін оңтайлы әдіс ұсынылды. Зерттелетін сызықты емес логикалық теңдеулер жүйелерінің класында логикалық формулалар кейбір сызықтық қосындыларға толығымен немесе ішінара бөлінеді. Нәтижесінде логикалық формулалар сызықтық көпмүшелердің көбейтіндісіне келтіріледі, оның негізінде екінші ретті логикалық теңдеулер жүйесіне қарағанда шама реті оңай шешілетін сызықтық логикалық теңдеулер жүйесі алынады және арнайы кластың екінші дәрежелі Жегалкин көпмүшелігінен алынған арнайы дизъюнктивтік қалыпты формалар үшін кейбір минимизациялау мәселелері қарастырылады.

Түйін сөздер: Жегалкин көпмүшесі, сызықтық логикалық функциялар, біртекті-бірлік матрицалар, көпмүшелік ұзындық, арнайы дизъюнктивті қалыпты формалар.

А.А. Байжуманов
Южно-Казахстанский государственный педагогический университет, Казахстан, Шымкент
e-mail: absattar52@mail.ru

Информационно-аналитическая система оценки состояния здоровья студентов

С целью упрощения обозначений и сокращения времени решения систем булевых уравнений предлагается метод, оптимальный для решения отдельного класса систем нелинейных булевых уравнений второй степени. В исследуемом классе систем нелинейных булевых уравнений логические формулы полностью или частично разбиваются на некоторые линейные множители. В результате логические формулы сводятся к произведению линейных многочленов, на основании чего получается система линейных булевых уравнений, которая решается на порядок проще, чем система булевых уравнений второго порядка и рассматривается некоторые задачи минимизации специальных дизъюнктивных нормальных форм, полученных из полинома Жегалкина второй степени специального класса.

Ключевые слова: многочлен Жегалкина, линейные булевы функции, однородно-единичные матрицы, полиномиальная длина, дизъюнктивные нормальные формы.

1 Introduction

Logical methods of recognition and methods of cryptanalysis, where systems of Boolean equations are used as mathematical models and their solution allows evaluating the solution of the corresponding applied problems. For example, the assessment of the cryptographic strength of cryptography algorithms in algebraic cryptanalysis is based on the analysis of solutions to systems of Boolean equations whose statements consist of Zhegalkin polynomials. Solving systems of Boolean equations are also used in logical pattern recognition. One of the parameters for assessing the cryptographic strength of encryption algorithms is the non - linearity of the Zhegalkin polynomials of statements of Boolean equations, which are elements of mathematical models for converting plain texts into cipher texts. Therefore, the problem under consideration in the article under study, where, by means of a transformation, second-order polynomials can be reduced to a product of first-order polynomials and, based on this transformation, we obtain a system of Boolean equations with first-order polynomials, is an actual problem in applied mathematics.

2 Problem statement

Let a system of nonlinear equations of the second degree:

$$\begin{cases} \sum_{i,j=1}^{n} a_{ij}^{(1)} x_i x_j \oplus \sum_{i=1}^{n} b_i^{(1)} x_i = \alpha_1 \\ \dots \qquad \dots \qquad \dots \\ \sum_{i,j=1}^{n} a_{ij}^{(m)} x_i x_j \oplus \sum_{i=1}^{n} b_i^{(m)} x_i = \alpha_m \end{cases} \tag{1}$$

where coefficients $\alpha_k, b_i^{(k)}, a_{ij}^{(k)} \in E_n^2 = \{0,1\}, k = \overline{1,m}; i,j = \overline{1,n}$; Moreover, $i \leq j$ and $x_i \cdot x_i = x_i$ takes place.

A compact representation of the notation of statements of a system of Boolean equations of the second degree is considered. In order to simplify the notation and reduce the time for solving the system of equations (1), a method is proposed that is optimal for solving a separate class of systems of nonlinear equations of the second degree. In such a class of systems of nonlinear equations, the propositions are completely or partially divided into some linear factors.

The idea of simplifying the writing of systems of equations (1) is to group elements $x_i \cdot x_j$ and selection of linear forms of the form $x_{i1} \oplus x_{i2} \oplus ... \oplus x_{ik}$, which are involved in various equations of the system.

Denote by $Y_{i_1,...i_k}$ the sum of $x_{i1} \oplus x_{i2} \oplus ... \oplus x_{ik}$: $Y_{i_1,...i_k} = x_{i1} \oplus x_{i2} \oplus ... \oplus x_{ik}$, here $1 \leq k \leq n; x_{ij} \in X^n = \{x_1, ..., x_n\}, 1 \leq j \leq k$.

It is easy to see that in system (1) there are many options for bracketing various sums $Y_{i_1,...i_k}$.

Example. Let

$$\begin{cases} x_1x_4 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_3x_5 = 1, \\ x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4 = 1. \end{cases}$$

After grouping elements x_i, x_j we have

$$\begin{cases}(x_1 \oplus x_2 \oplus x_3)(x_4 \oplus x_5) = 1,\\ (x_1 \oplus x_2 \oplus x_3)(x_1 \oplus x_4) = 1.\end{cases}$$

Introducing new variables

$$\begin{gathered}Y_{1,2,3} = x_1 \oplus x_2 \oplus x_3,\\ Y_{1,4} = x_1 \oplus x_4,\\ Y_{4,5} = x_4 \oplus x_5.\end{gathered}$$

We get the system

$$\begin{cases}Y_{1,2,3} \cdot Y_{4,5} = 1,\\ Y_{1,2,3} \cdot Y_{1,4} = 1.\end{cases}$$

From this we have

$$\begin{cases}Y_{1,2,3} = 1,\\ Y_{1,4} = 1,\\ Y_{4,5} = 1.\end{cases}$$

$$\begin{cases}x_1 \oplus x_2 \oplus x_3 = 1,\\ x_1 \oplus x_4 = 1,\\ x_4 \oplus x_5 = 1.\end{cases}$$

The solution is the set of sets:

$$\{10001\}, \{01010\}, \{00110\}, \{11101\}.$$

Let $\{Y\}$ be the set of all possible groupings in system (1). Let us assume that after some grouping of the elements of the statements of system (1) we have obtained

$$\begin{cases}\sum_{i,j=1}^{t} a_{ij}^{(1)} z_i z_j = \alpha_1\\ \ldots \qquad \ldots \qquad \ldots\\ \sum_{i,j=1}^{t} a_{ij}^{(m)} z_i z_j = \alpha_m\end{cases} \tag{2}$$

here $i \le j; z_i, z_j \in \{Y\}$; t is the cardinality of the set $\{Y\}$ used in system (2). The number $\Psi = \sum \varphi_Y |Y|$ is called the complexity of the system (2), where φ_Y is the number of $Y, Y \in \{Y\}$ participating in (2) and $|Y|$ is the number of elements in Y.

The task of grouping is to find among all possible systems (2) the one that gives the maximum φ_Y.

Each statement of the system of equations (1) can be specified separately as a matrix $||a_{ij}||_{n\times n}$ (Table 1).

a_{11}	a_{12}	a_{13}	...	a_{1n}
a_{21}	a_{22}	a_{23}	...	a_{2n}
.	.	.	...	.
a_{n1}	a_{n2}	a_{n3}	...	a_{nn}

In Table 1 $a_{ij} = 1$ if the terms $x_i x_j$ are involved in the corresponding equations of system (1), otherwise $a_{ij} = 0$.

3 Method for simplifying statements of a system of Boolean equations of the second degree

The method consists of two stages. From the beginning we prove the theorem of simplified representation of statements of the system of Boolean equations of the second degree. Next, we construct an algorithm for simplifying the notation of system (1).

Let $B = ||a_{ij}||_{n\times n}$ be the correspondence matrix of some equation of system (1).

Theorem 1. If a_{ij}, $i = i_1, ..., i_k$, $j = j_1, ..., j_t$ is a homogeneous identity submatrix of the matrix B corresponding to the statement $f(x_1, ..., x_n)$ from system (1), then

$f(x_1, ..., x_n) = Y_{i_1,...,i_k} \cdot Y_{j_1,...,j_t} \oplus f^2(x_1, ..., x_n)$.

Proof. Let the condition of the theorem be satisfied. Then it is easy to see that in B there are two uniformly symmetric submatrices a_{ij} and $b_{ji}(i = i_1, ..., i_k, j = j_1, ..., j_t)$, that have the same properties. Therefore, it is enough for us to consider one of them.

The existence of the submatrix a_{ij}, $i = i_1, ..., i_k$, $j = j_1, ..., j_t$ means that $f(x_1, ..., x_n)$ has the following factors:

$f^1 = x_{i1}x_{j1} \oplus x_{i1}x_{j2} \oplus ... \oplus x_{i1}x_{jt} \oplus x_{i2}x_{j1} \oplus x_{i2}x_{j2} \oplus ... \oplus x_{i2}x_{jt} \oplus ... \oplus x_{ik}x_{jt}$, that $f = f^1 \oplus f^2$.

Hence $f^1 = (x_{i1} \oplus x_{i2} \oplus ... \oplus x_{ik})(x_{j1} \oplus x_{j2} \oplus ... \oplus x_{jt}) = Y_{i_1,...,i_k} \cdot Y_{j_1,...,j_t}$.

Consequently $f = Y_{i_1,...,i_k} \cdot Y_{j_1,...,j_t} \oplus f^2$.

The theorem has been proven.

Corollary 1. If $a_{ij}^{\tau_1}$ $(i = i_1, ..., i_k,\ j = j_1, ..., j_t,\ \tau_1 = 1, ..., T_1)$, $b_{ln}^{\tau_2}$ $(l = l_1, ..., l_Q; n = n_1; \tau_2 = 1, ..., T_2\ )$, $c_{mr}^{\tau_3}$ $(m = m_1; r = r_1; \tau_3 = 1, ..., T_3)$ are all uniform-unit submatrices of the matrix B, then $f = (Y_{i_1,...,i_k} \cdot Y_{j_1,...,j_t})^{\tau 1} \oplus (x_{n1}Y_{l1...lQ})^{\tau 2} \oplus (x_{m1}x_{r1})^{\tau 3}$, where $T_1T_2T_3$ is the number of different groups.

Let $\{B\}$ be the set of all homogeneous-unit submatrices of the matrix B.

The algorithm for simplifying the notation of system (1) is built in two stages:

1st stage. Find $\widetilde{B} = \{B\}$ such that $|\widetilde{B}| = max|B'|$ where $B' \in \{B\}$, $|A|$ is the number of elements of the matrix A.

2nd stage. In the matrix B, we remove all elements of the submatrix $\widetilde{B}$.

If there are no identity elements in $\widetilde{B}$, then the algorithm terminates. Otherwise, go to the first stage.

Let, after running the algorithm, we obtain homogeneous-unit submatrices $B_1, B_2, ..., B_l$ where $\{B_1, B_2, ..., B_l\} = \{B\}$ and $|B_1| \geq |B_2| \geq ... \geq |B_l|$.

Hence, it is easy to see that, on the basis of Corollary 1, it is easy to construct an optimal grouping of elements of the statements of system (1).

Let L_J^2 and L_D^2 be the lengths (number of e.c.) of the second-degree Zhegalkin polynomial and its d.n.f., respectively. It is obvious that $L_J^2 \leq C_n^2 + n$, $L_D^2 \leq 2^{(C_n^2+n-1)}$.

If we denote by $L_{J_Y}^2$, $L_{D_Y}^2$ the lengths of the second degree Zhegalkin polynomial and its d.n.f. after running the simplification algorithm, it is easy to prove that $L_{J_Y}^2 \leq n$, $L_{D_Y}^2 \leq 2^{n-1}$ holds.

From here, it is easy to see that the problem of grouping elements reduces the maximum length of the Zhegalkin polynomial of the second degree by C_n^2 and reduces its d.n.f. $2^{(C_n^2)}$ times.

As a result of the algorithm, we obtain the system:

$$\begin{cases} \mathfrak{U}_1(x, Y(x)) = \alpha_1, \\ \dots \quad \dots \quad \dots \\ \mathfrak{U}_m(x, Y(x)) = \alpha_m. \end{cases}$$

where $\mathfrak{U}_i(x, Y(x))$ is the Zhegalkin polynomial of the second degree of grouped form ($i = \overline{1, m}$).

Let now $T = Y_{1,2,\dots,k} \cdot (Y_{1,2,\dots,k} \oplus Y_{k+1,\dots,t}) = 1$.

If there is a collection α such that $Y_{k+1,\dots,t}(\alpha) = 1$, then $T(\alpha) = 0$ is independent of the value of $Y_{1,2,\dots,k}(\alpha)$. Indeed, if $Y_{1,2,\dots,k}(\alpha) = 0$, then $T(\alpha) = 0(0 \oplus 1) = 0$. If $Y_{1,2,\dots,k}(\alpha) = 1$, then $T(\alpha) = 1(1 \oplus 1) = 0$.

$T(\alpha) = 1$ holds if and only if there exists a set α such that $Y_{1,2,\dots,k}(\alpha) = 1$ and $Y_{k+1,\dots,t}(\alpha) = 0$.

Consequently, the solution of equation (2) is solemnly the solution of the system

$$\begin{cases} Y_{1,2,\dots,k} = 1, \\ Y_{k+1,\dots,t} = 0 \end{cases}$$

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

Let G:

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

system of non-linear Boolean equations.

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

$$F_1(x_1, x_2, ..., x_n) = \sum_{i,j=k,i<j}^{k+3} a_{ij}x_ix_j \oplus \sum_{i,j=l,i<j}^{l+3} b_{ij}x_ix_j \oplus \sum_{i,j=p,i<j}^{p+3} c_{ij}x_ix_j \oplus \sum_{i,j=q,i<j}^{q+3} d_{ij}x_ix_j \oplus \sum_{i=t}^{t+3} e_ix_i,$$

where $k + 3 < l,\ l + 3 < p,\ p + 3 < q,\ q + 3 < t,$

$$\sum_{i,j=k}^{k+3} a_{ij} = \sum_{i,j=l}^{l+3} b_{ij} = \sum_{i,j=p}^{p+3} c_{ij} = \sum_{i,j=q}^{q+3} d_{ij} = 4, \qquad \{a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_i\} \in \{0, 1\}.$$

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

Here a sum of the form $\sum_{i,j=w}^{w+3} q_{ij}x_ix_j$ and $\sum_{i=v}^{v+3} e_ix_i$ 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_1 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 [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:

$$1)x_ix_j + x_ix_l + x_kx_j + x_lx_j = (x_i + x_j)(x_k + x_l) = Y_{ij}Y_{kl};$$
$$2)x_ix_j + x_ix_l + x_kx_i + x_ix_j = x_i(x_j + x_l + x_k) + x_kx_l = x_iY_{jlk} + x_kx_l;$$
$$3)x_ix_j + x_ix_l + x_ix_k + x_kx_l = x_i(x_j + x_l) + x_k(x_i + x_l) = x_iY_{jl} + x_kY_{il};$$

where $Y_{\nu_1\nu_2...\nu_z} = x_{\nu_1} + x_{\nu_2} + ... + x_{\nu_z}$.

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 $Y_{v_1v_2...v_z} = x_{v_1} + x_{v_2} + ... + x_{v_z}$ we have $Y_{v_1v_2...v_z} = z$.

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 [3] that for an arbitrary Zhegalkin polynomial $Q(x_1, x_2, ..., x_n) = U_1 + U_2 + ... + U_t$ where U_i are elementary conjunctions, $i = \overline{1,t}$ we have the equality

$$Q(x_1, x_2, ..., x_n) = \vee_{\sigma_1+\sigma_2+...+\sigma_t=1} U_1^{\sigma_1} \ \& \ U_2^{\sigma_2} \ \& \ ... \ \& \ U_t^{\sigma_t} \tag{3}$$

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 (3), 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:

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

where $m < 10, l \leq 18, z_i, z_i^{'} \in \{x_1, x_2, ..., x_n\}, \{Y_{v,w}\}; |v - \underline{w}| \leq 3;$

$v, w = \{1, 2, ..., n\}, U_i = z_i z_i^{'}; z_i z_i^{'} \in \{z_1, z_2, ..., z_l\}, i = \overline{1, m}.$

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 [3] $(a_i b_i)$ c.c. $U_i (i = \overline{1, m})$.

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

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

2) For each conjunction $U_1^{\sigma^1}, U_2^{\sigma^2}, ..., U_m^{\sigma^m}$ in disjunction

$$F(z_1, z_2, ..., z_l) = \vee_{\sigma_1 + \sigma_2 + ... + \sigma_t = 1} U_1^{\sigma_1} \ \& \ U_2^{\sigma_2} \ \& \ ... \ \& \ U_t^{\sigma_t},$$

where $\sigma_i \in \{0, 1\}, i = \overline{1, m}$, we write out all the unit coordinates $(\sigma_{i_1}, \sigma_{i_2}, ..., \sigma_{i_k})$ of the set $(\sigma_1, \sigma_2, ..., \sigma_m)$. With the help of $(b_{i1}, b_{i2}, ..., b_{ik})$ we calculate the decimal representation of the conjunction $(U_{i1}, U_{i2}, ..., U_{ik})$. For the zero coordinates $\sigma_{ij} (j = \overline{k+1, m})$ of the set $(\sigma_1, \sigma_2, ..., \sigma_m)$ we write out c_{ij}, which are decimal representations of the c.c. $U_{ij} = z_i z_k$. 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. $\neg z_i$ and $\neg z_k$;

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

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

5 Finding the roots of a system of nonlinear equations of the second degree

Let

$$\begin{cases} U_{11} \vee U_{12} \vee ... \vee ...U_{1n_1} = 1; \\ U_{21} \vee U_{22} \vee ... \vee ...U_{2n_2} = 1; \\ \quad ... \quad ... \quad ... \\ U_{m1} \vee U_{m2} \vee ... \vee ...U_{mn_m} = 1. \end{cases} \tag{4}$$

The system of equations, where complex conjunctions (c.c.) $U_{ij}, i = \overline{1, m}; j = \overline{1, n_i}$ has the form: $x_{i_1}^{\sigma_1} ... x_{i_k}^{\sigma_k} Y_{v_1 ... v_{t_1}}^{\sigma_{k+1}} ... Y_{w_1 ... w_{t_l}}^{\sigma_{k+l}}$. It is easy to see that if $\wedge_{k=1}^{m} U_{kj_k} \neq 0$, $(j_k \in \{1, 2, ..., n_k\})$, $k = \overline{1, n}$ then the solution of the equation

$$\wedge_{k=1}^{m} U_{kj_k} = 1 \tag{5}$$

is the solution of system (4).

Obviously, applying transformations: $x_i^{\sigma_i} \cdot x_i^{\sigma_i} = x_i^{\sigma_i}$; $\quad Y^{\sigma_i}_{v_1...v_t} Y^{\sigma_i}_{v_1...v_t} = Y^{\sigma_i}_{v_1...v_t}$;

$$x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} \;\; Y^{\sigma}_{i_1...i_l} = 0, \quad \text{at} \sum_{i=1}^{l} \sigma_i = \bar{\sigma}, \text{where the symbol} \sum \text{means the sum modulo 2;}$$

$$x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} \;\; Y^{\sigma}_{i_1...i_l} = x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l}, \quad \text{at} \sum_{i=1}^{l} \sigma_i = \sigma;$$

$$x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} \;\; Y^{\sigma}_{i_1...i_{l+1}} = x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l}\overline{(x)}_{i_{l+1}}, \quad \text{at} \sum_{i=1}^{l} \sigma_i = \sigma;$$

$$x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} \;\; Y^{\sigma}_{i_1...i_{l+1}} = x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} x_{i_{l+1}}, \quad \text{at} \sum_{i=1}^{l} \sigma_i = \bar{\sigma};$$

$$x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} \;\; Y^{\sigma'}_{i_1..i_{l+1}..i_k} = x^{\sigma_1}_{i_1}...x^{\sigma_l}_{i_l} x^{\sigma''}_{i_{l+1}..j_k}, \quad \text{at} \sum_{i=1}^{l} \sigma_i + \sigma' = \sigma'';$$

$$Y^{\sigma_1}_{i_1..i_k} \; Y^{\sigma_2}_{i_1..i_k i_{k+1}..i_m} = Y^{\sigma_1}_{i_1..i_k} \; Y^{\sigma_1 \oplus \sigma_2}_{i_{k+1}..i_m}, (\sigma_j \in \{0,1\}, j \in \{1,2,...,n\})$$

equation (5) can be reduced to the form: $x^{\delta_1}_{j_1}...x^{\delta_t}_{j_t} \; Y^{\delta_{t+1}}_{p_1...p_{k_1}}...Y^{\delta_{t+l}}_{q_1...q_{k_l}} = 1$.

Moreover, this equation is equivalent to the system of linear equations:

$$\begin{cases} x_{j_1} = \delta_1 \\ \quad ... \quad\quad ... \\ x_{j_t} = \delta_t \\ Y_{p_1...p_{k_1}} = \delta_{t+1} \\ \quad ... \quad\quad ... \\ Y_{q_1...q_{k_l}} = \delta_{t+l} \end{cases} \tag{6}$$

where $Y_{v_1...v_{k_l}} = x_{v_1} \oplus x_{v_2} \oplus ... \oplus x_{v_t}$. Thus, system (6) is equivalent to equation (5) and its solution will satisfy system (4).

The algorithm for solving system (4) is as follows. For all c.c. $U_{11}, U_{12}, ..., U_{mn_m}$ such that the product $\wedge_{k=1}^{m} U_{kj_k}$ does not contain the elements z^{σ} and $z^{\bar{\sigma}}$, where $z = x_i$ or $z = Y_{v_1...v_t}$, we construct the equation $\wedge_{k=1}^{m} U_{kj_k} = 1$. The resulting equation is reduced to a system of linear equations. We find its solution by the method of elimination of variables. The result of the algorithm will be the solution of joint systems of linear equations that satisfies the system (4).

The general scheme for solving a system of Boolean equations is as follows:

SYSTEM OF BOOLEAN EQUATIONS
↓
GROUPING OF STATEMENT ELEMENTS
↓
CONVERSION OF THE SYSTEM'S STATEMENTS FOR SPECIAL D.N.F.
↓
MULTIPLICATION OF COMPLEX CONJUNCTIONS
↓
MINIMIZATION OF SPECIAL D.N.F.

Conclusion

In order to simplify the notation and reduce the time for solving systems of Boolean equations, a method is proposed that is optimal for solving a separate class of systems of non-linear Boolean equations of the second degree.

A theorem is proved that in the class of systems of non-linear Boolean equations of the second degree under study, logical formulas are divided completely or partially into some linear factors. A method is proposed for reducing logical formulas to a product of linear polynomials, on the basis of which a system of linear Boolean equations is obtained, which is solved an order of magnitude easier than a system of second-order Boolean equations. It is proved that the problem of grouping elements reduces the maximum length of the second degree Zhegalkin polynomial by C_n^2 and reduces its d.n.f. $2^{(C_n^2)}$ times.

References

[1] A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security,"2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746

[2] A. Kabulov, I. Saymanov, I. Yarashov and A. Karimov, "Using Algorithmic Modeling to Control User Access Based on Functioning Table,"2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850

[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. Glavnayaredaksiyafiziko-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 satisfiability (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.