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

METHODS FOR SOLVING SYSTEMS OF BOOLEAN EQUATIONS

Abdussattar Abdukadirovich BAYZHUMANOV [1]

ABSTRACT

To minimize logical formulas when solving systems of Boolean equations, a method is proposed for transforming formulas from the Zhegalkin polynomial into a disjunctive normal form. Algorithms for simplifying logical functions in the class of disjunctive normal forms are given. A method for multiplying logical expressions in the class of disjunctive normal forms is proposed. Neighborhoods of the 1st order of disjunctive normal forms of complex conjunctions of logical of manifestations of systems of nonlinear Boolean equations given by Zhegalkin polynomials. A method is proposed for minimizing disjunctive normal forms based on the absorption of complex conjunctions by a first-order neighborhood. For this, criteria for the absorption of complex conjunctions by a first-order neighborhood are proved, similarly to the theory of Yu.I. Zhuravlev on the absorption of elementary conjunctions in the class of disjunctive normal forms of Boolean functions. Four algorithms for minimizing disjunctive normal forms of complex conjunctions based on a neighborhood of the 1st order have been developed. As a result, the logical formulas are reduced to the product of the formulations of the Boolean equations of the system, from which the solutions of the system of Boolean equations are obtained. At the end, an estimate of the complexity of the algorithm for solving systems of Boolean equations is given.

Keywords: Zhegalkin polynomial, linear Boolean functions, polynomial length, disjunctive normal forms, first-order neighborhood, metric characteristic.

---

[1] 1south Kazakhstan State Pedagogical University, Faculty of Physics and Mathematics, Mathematics Department, Shymkent, ORCID: 0009-0007-1309-548, absattar52@mail.ru
Araştırma Makalesi/Research Article, Geliş Tarihi/Received: 25/04/2023–Kabul Tarihi/Accepted: 12/05/2023

BOOLE DENKLEMLERİNİN SİSTEMLERİNİ ÇÖZME YÖNTEMLERİ

ÖZET

Boole denklem sistemlerini çözerken mantıksal formülleri en aza indirmek için, formülleri Zhegalkin polinomundan ayrık normal forma dönüştürmek için bir yöntem önerilmiştir. Ayırıcı normal formlar sınıfında mantıksal fonksiyonları basitleştirmek için algoritmalar verilmiştir. Ayrık normal formlar sınıfındaki mantıksal ifadeleri çarpmak için bir yöntem önerilmiştir. Mantıksal karmaşık bağlaçların ayrık normal biçimlerinin 1. dereceden komşulukları Zhegalkin polinomları tarafından verilen doğrusal olmayan Boole denklem sistemlerinin göstergelerindendir. Karmaşık bağlaçların birinci dereceden bir komşuluk tarafından soğurulmasına dayalı ayrık normal formları en aza indirmek için bir yöntem önerilmiştir. Bunun için, karmaşık bağlaçların birinci dereceden bir komşuluk tarafından emilmesi için kriterler, Yu.I. Zhuravlev, Boolean fonksiyonlarının ayrık normal biçimleri sınıfındaki temel bağlaçların özümsenmesi üzerine. 1. dereceden bir komşuluğa dayanan karmaşık bağlaçların ayrık normal biçimlerini en aza indirmek için dört algoritma geliştirilmiştir. Sonuç olarak, mantıksal formüller, Boole denklemleri sisteminin çözümlerinin elde edildiği sistemin Boole denklemlerinin formülasyonlarının ürününe indirgenir. Sonunda, Boole denklem sistemlerini çözmek için algoritmanın karmaşıklığının bir tahmini verilir.

Anahtar Kelimeler: Zhegalkin polinomu, doğrusal Boole fonksiyonları, polinom uzunluğu, ayrık normal formlar, birinci dereceden komşuluk, metrik karakteristik

INTRODUCTION

In logical recognition systems, logical methods based on discrete analysis and propositional calculus based on it are used to construct recognition algorithms proper. In the general case, the logical recognition method provides for the presence of logical connections expressed through a system of Boolean equations, in which the variables are the logical features of the objects or phenomena being recognized.

The logical signs of recognizable objects can be considered as elementary statements that take two truth values: true and false.

First of all, logical signs include signs that do not have a quantitative expression. These signs are judgments of a qualitative nature (the presence or absence of certain properties or certain elements of recognizable objects or phenomena). Logical signs, for example, in medical diagnostics, may be the following symptoms: sore throat, cough, runny nose, etc. The engine type of the recognizable aircraft - jet, turboprop or piston - can also be considered as a logical feature. In geology, logical signs can be solubility or insolubility in certain acids or in certain mixtures of acids, the presence or absence of odor, color, etc.

The number of logical features can also include features that have a quantitative expression; however, it is important (and taken into account) not in itself the value of the feature of the recognized object, but only the fact that it falls or does not fall into a given interval. In practice, logical features of this kind take place in situations where measurement errors can either be neglected, or the intervals of feature values are chosen in such a way that measurement errors practically do not affect the reliability of decisions made regarding whether the measured quantity falls within a given interval.

A new area of application of the methods of algebra of logic, which has emerged recently, is the problem of recognizing a set of objects and phenomena, which can be reduced to solving systems of logical equations. This paper describes the basic principles for solving systems of logical equations and constructs algorithms for obtaining solutions to the maximum joint subsystems of Boolean equations.

1. SOLUTION OF SYSTEMS OF BOOLEAN NONLINEAR EQUATIONS

Let a system of nonlinear Boolean equations be given, the statements of which consist of disjunctive normal forms (d.n.f.):

$$\begin{array}{l} U_{11} \vee U_{12} \vee \ldots \vee U_{1l_1} = 1 \\ U_{21} \vee U_{22} \vee \ldots \vee U_{2l_2} = 1 \\ \ldots \\ U_{m1} \vee U_{m2} \vee \ldots \vee U_{ml_m} = 1 \end{array} \qquad (1)$$

where

$$U_{ij} = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \ldots x_{i_k}^{\delta_k}$$

It is easy to see that the binary set ά is a solution to system (2.1) if and only if there exists an equation

$$U_{1,i_1} \& U_{2,i_2} \& \ldots \& U_{\mathrm{m},i_m} = 1 \qquad (2)$$

for which $\tilde{\alpha}$ is the solution.

Let the system of logical equations be given in the basis $D_2 = \{1, \mathrm{x}_1 + \mathrm{x}_2, \mathrm{x}_1 \wedge \mathrm{x}_2\}$ in the form of the Zhegalkin polynomial:

$$\begin{cases} f_1 = \sum_{j=1}^{k_1} A_{1j} = L_1 \\ \ldots \\ f_m = \sum_{j=1}^{k_m} A_{mj} = L_m \end{cases} \qquad (3)$$

where A_{ij} -elementary conjunction; $L_i \in \{0,1\}; \mathrm{i}=1,\ldots,\mathrm{m}; \mathrm{j}=1,\ldots,\mathrm{k}_i$.

Each statement of the equations of system (3) is transformed into a d.n.f. using the following formulas:

a) for $n = 2k + 1$

n n n-1 n n-3 n-2 n-1 n

$\sum A_i = \& A_i \vee V V (B_{ji} \& \neg A_j \& \neg A_i) \vee V V V V (B_{jtli} \&$

i=1 i=1 j=1 i=j+1 j=1 t=j+1l=t+1i=l+1

n-k1+1 n-k1+2 n

$\& \neg A_j \neg A_t \neg A_l \neg A_i) \vee \ldots \vee V V \ldots V (B_{jt\ldots i} \neg A_j \neg A_t \ldots \neg A_i),$

j=1 t=j+1 i=l+1

b) for $n = 2k$

$$\sum_{i=1}^{n} A_i = \bigvee_{i=1}^{n} (B_i \neg A_i) \vee \bigvee_{i=1}^{n-2} \bigvee_{j=i+1}^{n-1} \bigvee_{t=j+1}^{n} (B_{ijt} \neg A_i \neg A_j \neg A_t) \vee \ldots \vee \bigvee_{i=1}^{n-k+1} \bigvee_{j=i+1}^{n-k+2} \ldots \bigvee_{t=l+1}^{n} (\mathrm{B}_{ij\ldots t} \neg A_i \neg A_j \ldots \neg A_t),$$

and identities:

$$\neg(\mathrm{A}_1 \wedge \mathrm{A}_2 \wedge \ldots \wedge \mathrm{A}_e) = \neg \mathrm{A}_1 \vee \neg \mathrm{A}_2 \vee \ldots \vee \neg \mathrm{A}_e,$$

$$\neg(\mathrm{A}_1 \vee \mathrm{A}_2 \vee \ldots \vee \mathrm{A}_e) = \neg \mathrm{A}_1 \wedge \neg \mathrm{A}_2 \wedge \ldots \wedge \neg \mathrm{A}_e,$$

$$\mathrm{A} \wedge (\mathrm{A}_1 \vee \mathrm{A}_2 \vee \ldots \vee \mathrm{A}_e) = \mathrm{A}_1 \wedge A \vee \ldots \mathrm{A}_2 \wedge A \vee \ldots \vee A_e \wedge A$$

Here, each d.n.f. simplified step by step with the following logical operations:

$$\neg A \wedge A = 0; 0 \wedge A = 0; 0 \vee A = A;$$

$$A \vee A = A; 1 \wedge A = A; A \wedge A = A;$$

$$\neg A \forall A = 1; 1 \forall A = 1;$$

$$A \vee A \wedge B = A; A \wedge \neg x \vee A \wedge x = A.$$

It is easy to see that as a result we obtain a system of equations:

$$\begin{cases} D_1 = U_{11} \vee \ldots \vee U_{1t_1} = 1 \\ D_2 = U_{21} \vee \ldots \vee U_{2t_2} = 1 \\ \ldots \\ D_m = U_{m1} \vee \ldots \vee U_{mt_m} = 1 \end{cases} \qquad (4)$$

where U_{ij} -elementary conjunction; $\mathrm{i} = 1, \ldots, \mathrm{m}$; $\mathrm{j} = 1, \ldots, \mathrm{t}_i$, $D_i -$ abbreviated d.n.f. , realizing $f_i, i = 1, \ldots, m.$

2 METHOD OF MULTIPLICATION OF DISJUNCTIVE NORMAL FORMS

Let us reduce systems (4) to one equivalent equation

D1 _&D $_2$ &… &D $_m$ =1 , in which the left-hand side is represented as a d.n.f.:

K_1 v K_2 v … v K_t = 1,

where K_i – e.c. , i=1,…,t .

It is easy to see that

U^($\mathbf{V}_{i=1}^{t}$U $_{ij}$) = U ,

Then and only when

(U→$\mathbf{V}_{j=1}^{k}$U $_{ij}$) = 1 ,

where U, U_i – e.c. i=k; {U $_{i1}$,…,U $_{ik}$ } ∈{U $_1$,…,U $_t$ }.

Let

$D_1 = U_1$vU_2 v … v U_{m1} = 1,

$D_2 = U^1{}_1$ v $U^1{}_2$ v … v$U^1{}_{m2}$=1, (5)

equations of system (3).

Through χ (D $_1$ &D $_2$) we denote the length of the products D $_1$ &D $_2$, in which it is known that χ (D $_1$ &D $_2$)=m $_1$ ·m $_2$.

It is easy to see that if $U_i = U_j{}^1$, then

D1& D2 = U $_i$v ($\mathbf{V}_{\tau=1,\tau\neq i}^{m_1}$U $_i$)($\mathbf{V}_{t=1,t\neq j}^{m_2}$U $_t$),

χ (D$_1$ &D $_2$) = 1+ (m $_1$ -1)(m $_2$ -1).

Lemma. If in d.n.f.D1 and _D2 _occurs

$$U_{i_1} = Ax^{\sigma}, U^1_{j_1} = Ax^{\neg\sigma}, \sigma = \{0,1\},$$

$$\left(U_{i_1} \to U^1_{j_t}\right) = 1, \left(U^1_{j_1} \to U_{i_t}\right) = 1, \text{then} U_{i_t} \wedge U^1_{j_1} = 0.$$

<u>Proof</u> . The case $U_{i_t} \wedge U^1_{j_1}$ is obvious. By condition $\left(U_{j_1} \to U_{i_t}\right) = 1$ we have $\left(Ax^{\sigma} \to U_{i_t}\right) = 1$. Suppose that $U_{i_t} = A_1$, where $\left(A \to A_1\right) = 1$, while the condition $\left(U_{j_t} \to U_{i_t}\right) = 1$ is true. Then $U_{i_1} \vee U_{i_t} = A_1$. This cannot be, since D_1 is an abbreviated d.n.f. Therefore, it must be $U_{i_t} = Ax^{\bar{\sigma}}$, then $\left(Ax^{\bar{\sigma}} \to A_1 x^{\bar{\sigma}}\right) = 1$, (where $\left(A \to A_1\right) = 1$) takes place, and e.c. U i1 , U it does not cancel, which corresponds to the condition of the lemma. From the same considerations, we can get that $U^1_{j_t} = Ax^{\sigma}$, where $A \to A_2 = 1$, and therefore , we have

$$U_{i_t} \wedge U^1_{j_t} = A_1 x^{\bar{\sigma}} \wedge A_2 x^{\sigma} = 0 .$$

The lemma is proven.

<u>Theorem</u> . If in d.n.f. D_1 and D_2 :

$$U_{i_1} = Ax^{\sigma}, U^1_{j_1} = Ax^{\neg\sigma}, x \in \{x_1, ..., x_n\}, \sigma = \{0,1\},$$

$$\left(U_{i_1} \to U^1_{j_{t_1}}\right) = 1, \left(U^1_{j_1} \to U_{i_1}\right) = 1,$$

$$\left(U_{i\,k_q} \to A\right) = 1, \left(U^1_{j\,n_\gamma} \to A\right) = 1,$$

$q = \overline{1,l}; \gamma = \overline{1,m}.$,then the following is true :

$$D_1 \,\&\, D_2 = A \vee \left(\mathop{\vee}_{r=2, r\neq ka}^{m_1} U_{i_t} \right) \left(\mathop{\vee}_{t=2, t\neq n\gamma}^{m_2} U_{j_t} \right)$$

$$\chi\left(D_1 \,\&\, D_2\right) = (m_1 - l - 1)(m_2 - m - 1) .$$

<u>Proof</u> . Let's rewrite the system (5) as follows :

$$D_2 = U^1_{j_1} \vee U^1_{j_{t_1}} \vee \left(\mathop{\vee}_{\gamma=1}^{m} U^1_{j_{n\partial}} \right) \vee \left(\mathop{\vee}_{t=2, t\neq n\partial, t\neq t_1}^{m_2} U^1_{j_t} \right).$$

According to the statements (4) , (5) and the lemma, under the condition of the theorem, the following identities are true:

$$U_{i_1} \wedge U^1_{j_t} = U_{i_1}, U_{i_\tau} \wedge U^1_{j_1} = U^1_{j}, U_{j_1} \wedge U^1_{j_1} = 0,$$

$$U_{i_{\tau 1}} \wedge U^1_{j_{t1}} = 0, U_{i_1} \vee U^1_{j_1} = A,$$

$$U_{i k_q} \wedge \left[\left(\mathop{\vee}_{\partial=1}^{m_1} U^1_{j_{n\partial}} \right) \vee \left(\mathop{\vee}_{t=2, t \neq n\partial}^{m_2} U^1_{j_t} \right) \right] \to A = 1,\ q = \overline{1, l};$$

$$U^1_{j_{n\gamma}} \wedge \left[\left(\mathop{\vee}_{q=1}^{l} U_{i_{kq}} \right) \vee \left(\mathop{\vee}_{\tau=2, \tau \neq kq}^{m_1} U_{i_\tau} \right) \right] \to A = 1,\ \gamma = \overline{1, m}.$$

Therefore, the product $D_1 \,\&\, D_2$ can be written as:

$$D_1 \,\&\, D_2 = A \vee \left(\mathop{\vee}_{\tau=2, \tau \neq kq}^{m_1} U_{i_\tau} \right) \left(\mathop{\vee}_{t=2, t \neq n\gamma}^{m_2} U^1_{j_t} \right)$$

Taking into account (4) and $U_{i_{\tau 1}} \wedge U^1_{j_{t1}} = 0$, we have:

$$\chi\left(D_1 \,\&\, D_2\right) = (m_1 - l - 1)(m_2 - m - 1).$$

The theorem has been proven.

Methods for reducing d.n.f. special kind.

On the basis of the considered statements and the theorem, we construct algorithms $A1, A2, A3, A4$.

Algorithm A1.

1. Check the conditions:

$$U_{i_1} = Ax^{\sigma},\ U^1_{j_1} = Ax^{\neg\sigma},\ \left(U_{i_1} \to U^1_{j_t}\right) = 1,\ t = 2, \ldots, m_2;$$
$$\left(U^1_{j_1} \to U_{i_\tau}\right) = 1,\ \tau = 2, \ldots, m_1 \ (6)$$

Let us assume that etc. $U_{i_1}, U^1_{j_1}$ satisfies condition (6), then $U_{i_1} \vee U^1_{\neg j_1} = A$ takes place.

1. Let us consider such e.c., which
   $U_{i_v} = U^1_{j_v}$ (7)

If a

$$U^1_{j_v} = U_{i_v} = A_1 x^{\sigma}, A = A_1 x^{\sigma}, \sigma \in \{0,1\} \ (8),$$

then U_{i_ν} and $U^1_{j_\nu}$ excluded from D_1 and D_2, respectively. e.c. A_1 we write in place A and repeat step 2 if conditions (7) and (8) are again satisfied, otherwise we go to the next step.

3. Check the absorption conditions for the remaining e.c. from D_1 and D_2. Let the following take place:

$$\left(U_{ik_q} \to A\right) = 1,\ q = \overline{1,l};$$

$$\left(U^1_{jn_\gamma} \to A\right) = 1,\ \gamma = \overline{1,m}. \quad (9)$$

Then e.c. U_{ik_q} and $U^1_{jn_\gamma}$ excluded from the D.N.F. D_1 and D_2. It is obvious that by successively applying this algorithm , we can eliminate the set of e.c. from d.n.f. D_1 and D_2.

Let q be the number of pairs of e.c. satisfying conditions (8) and (9) . Then , according to the theorem, we have

$$D_1 \,\&\, D_2 = A_{i_1} \vee A_{i_2} \vee \ldots \vee A_{i_q} \vee \left(\bigvee_{\tau=q+g+1}^{m_1} U_{i_\tau}\right)\left(\bigvee_{\tau=q+\gamma+1}^{m_2} U^1_{j_t}\right),$$

where $A_{i_k} \in \left(U_{i_k}, U^1_{j_k}\right),\ k = \overline{1,q};\ g$ and γ are the number of excess e.c. from d.s.f. D_1 and D_2 by condition (11) and

$$\chi\left(D_1 \,\&\, D_2\right) = q + (m_1 - q - g)(m_2 - q - \gamma) - q = (m_1 - q - g)(m_2 - q - \gamma).$$

Algorithm A2.

For e.c. $U_{i\tau}, \tau = q + g + 1, \ldots, m_1;\ U^1_{jt}, t = q + \gamma + 1,\ U^1_{jt}, t = q + \gamma + 1, \ldots, \mathrm{m}_2$ we check the conditions $U_{i\tau} = U^1_{jy}$.

Let $U_{i_{q+g+1}} = U^1_{j_{q+\gamma+1}}, \ldots, U^1_{j_{q+g+1}} = U^1_{j_{q+\gamma+1}}$.

Then , according to (6) , the following is true:

$$D_1 \,\&\, D_2 = A_{i_1} \vee \ldots \vee A_{i_q} \vee U_{i_{q+g+1}} \vee \ldots \vee U_{i_{q+g+l}} \vee$$

$$\ldots \vee \left(\bigvee_{\tau=q+g+l+1}^{m_1} U_{i_\tau}\right)\left(\bigvee_{\tau=q+\gamma+l+1}^{m_2} U^1_{j_t}\right)$$

$$\chi\left(D_1 \,\&\, D_2\right) = q + l + \left(m_1 - q - g - 1\right)\left(m_2 - q - \gamma - 1\right).$$

Algorithm A3.

Now for e.c. U_{i_τ} and $U^1_{j_t}, \tau = q+g+l+1,\dots,\mathrm{m}_1;\ t = q+\gamma+l+1,\dots,m_2$ check the conditions: $\left(U_{i_\tau} \to U^1_{j_t}\right)=1, \left(U_{i_\tau} \to \bigvee_{t_1=l_1}^{m_2} U^1_{j_{t_1}}\right)=1$, where $q+\gamma+l+1 \le l_1,\ m^1_2 \le m_2,\ l_1 \le m^1_2$.

Let $k-$be the number of e.c. from U_{i_τ}, which absorb e.c. $U^1_{j_t}$. Then, according to (3) and (4) , absorbed e.c. can be derived from multiplication. We will assume that these e.c. are $U_{i_{q+g+l+1}},\dots,U_{i_{q+g+l+k}}$. Then in the product we get:

$$D_1 \,\&\, D_2 = A_{i_1} \vee A_{i_2} \vee \dots \vee A_{i_q} \vee U_{i_{q+g+l}} \vee U_{i_{q+g+l+1}} \vee$$

$$\vee \dots \vee U_{i_{q+g+l+k}} \vee \left(\bigvee_{\tau=q+g+l+k+1}^{m_1} U_{i_\tau}\right)\left(\bigvee_{t=q+\gamma+l+1}^{m_2}\right)$$

$$\chi\left(D_1 \,\&\, D_2\right) = q+l+k+\left[m_1-\left(q+g+l+k\right)\right]\left[m_2-\left(q+\gamma+l\right)\right].$$

Algorithm A4.

This algorithm checks the conditions of Algorithm A3 for e.c. $U^1_{j_t},\ t = q+\gamma+l+1,\dots,m_2$ with e.c. $U_{i_\tau}, \tau = q+g+l+k+1,\dots,m_1$.

Suppose there are m absorbed e.c. As in the A3 algorithm, we write the product as follows:

$$D_1 \,\&\, D_2 = A_{i_1} \vee \dots \vee A_{i_q} \vee U_{i_{q+g+1}} \vee U_{i_{q+g+l+1}} \vee \dots \vee U_{i_{q+g+l+k}} \vee$$

$$\vee U^1_{j_{q+\gamma+l+1}} \vee \dots \vee U^1_{j_{q+\gamma+l+m}} \vee \left(\bigvee_{\tau=q+g+l+k+1}^{m_1} U_{i_\tau}\right)\left(\bigvee_{\tau=q+\gamma+l+m+1}^{m_2} U^1_{j_t}\right)$$

$$\chi\left(D_1 \,\&\, D_2\right) = q+l+k+m+\left[m_1-\left(q+g+l+k\right)\right]\left[m_2-\left(q+\gamma+l+m\right)\right]$$

Let

$$D = A_{i_1} \vee A_{i_2} \vee \dots \vee A_{i_q} \vee U_{i_{q+g+1}} \vee \dots \vee U_{i_{q+g+l}} \vee U_{i_{q+g+l+1}} \vee$$

$$\vee \dots \vee U_{i_{q+g+l+k}} \vee U^1_{i_{q+\gamma+l+1}} \vee U^1_{i_{q+\gamma+l+m}}$$

- part of the product obtained using algorithms A1,A2 , A3, A4 .

We introduce the notation $\neg P\left(U,G\right)$ and $\neg S\left(U,G\right)$, respectively, that e.c. U and G do not absorb each other and do not stick together.

Theorem. V d.n.f $D, \neg P\left(U_i, U_j\right), \neg S\left(U_i, U_j\right)$,

where U_i, U_j are elementary conjunctions from D, $i \neq j$.

Proof. It is known that d.n.f. D_1 and D_2 are abbreviated. It is easy to see that in D there are four groups of e.c. obtained using algorithms A1, A2, A3 and A4:

$\left\{A_{i_1}, \ldots, A_{i_q}\right\}, \left\{U_{i_{q+g+1}}, \ldots, U_{i_{q+g+1}}\right\}, \left\{U_{i_{q+g+l+1}}, \ldots, U_{i_{q+g+l+k}}\right\}$,

$\left\{U^1_{j_{q+\gamma+l+1}}, \ldots, U^1_{j_{q+\gamma+l+m}}\right\}$, for which it is required to prove the assertion of the theorem.

Occurs $\neg P\left(A_{i_v}, U_{i_w}\right), \neg S\left(A_{i_v}, U_{i_w}\right), \neg P\left(A_{i_v}, U^1_{j_t}\right), \neg S\left(A_{i_v}, U^1_{j_t}\right)$,

where $v = 1, \ldots, q;\ \mathrm{w} = \mathrm{q} + \mathrm{g} + 1, \ldots, \mathrm{q} + \mathrm{g} + \mathrm{l} + \mathrm{k};\ \mathrm{t} = \mathrm{q} + \gamma + \mathrm{l} + 1, \ldots, \mathrm{q} + \gamma + \mathrm{l} + \mathrm{m}$,

since according to Algorithm A1 all e.c. for which the operations of absorption and gluing are valid are removed.

Now we also have

$\neg P\left(U_{i_v}, U_{i_w}\right), \neg S\left(U_{i_v}, U_{i_w}\right), \neg P\left(U_{i_v}, U^1_{j_t}\right), \neg S\left(U_{i_v}, U^1_{j_t}\right)$,

¬ P(Ui v , Ui w), ¬ S(Ui v , Ui w), ¬ P(Ui v , U 1 j t), ¬ S(Ui v , U 1 j t),where $v = q + g + 1, \ldots, q + g + l$; $w = q + g + l + 1, \ldots, q + g + l + k$; $t = q + \gamma + l + 1, \ldots, q + \gamma + l + m$,

we have from the fact that U_{i_v}, U_{i_w} are elementary conjunctions from D_1 and $U_{i_v} = U^1_{j_{t_1}}$, $t_1 = q + \gamma + 1, \ldots, \mathrm{q} + \gamma + l$; $\mathrm{U}^1_{j_{t_1}}, \mathrm{U}^1_{j_t}$ – e. l.D2.

Now it remains to prove that $\neg P\left(U_{i_v}, U^1_{j_t}\right), \neg S\left(U_{i_v}, U^1_{j_t}\right), v = q + g + l + 1, \ldots, q + g + l + k$; $t = q + \gamma + l + 1, \ldots, q + \gamma + l + m$.

Let $\left(U_{d_1} \to U^1_{d_2}\right) \equiv 1$, $U_{d_1} \in U_{i_\tau}$, $U^1_{d_2} \in U^1_{j_t}$.

According to the A3m algorithm, we have $\left(U^1_{d_2} \to U\right) \equiv 1$, where U is an e.c. from D1. Then we have $\left(U_{d_1} \to U\right) \equiv 1$. But this cannot be, since U_{d_1}, U are elementary conjunctions from the abbreviated dnf D_1. Thus does not hold and $\left(U^1_{d_2} \to U^1_{d_1}\right) \equiv 1$. The assumption is wrong and hence it follows that $\neg P\left(U_{i_\tau}, U^1_{j_t}\right)$. The statement $\neg S\left(U_{i_\tau}, U^1_{j_t}\right)$ is true, since all gluing of e.c. excluded from D1 and D2 according to Algorithm A1

The theorem has been proven.

Note that in the case of changing the order of implementations of Algorithm A1 with others, the statements of the previous theorem may be incorrect and, therefore, the implementation of the algorithms is optimal when Algorithm A1 is executed first.

It is easy to see that to obtain the result of the product $D1\&D2$, it will only be necessary to multiply and reduce an insignificant number of e.c. d.s.f. $D1$ and $D2:\left(V_{\tau=q+g+l+k+1}^{m_1}U_{i_\tau}\right),\left(V_{t=q+\gamma+l+m+1}^{m_2}U_{j_t}^{1}\right),$

For which the estimate

$$\chi_1\left(D_1\&D_2\right)=\left[m_1-\left(q+g+l+k\right)\right]\left[m_2-\left(q+\gamma+l+m\right)\right]$$

and if $q+g+l+k=m_1$ or $q+\gamma+l+m=m_2$, then $\chi_1(\mathrm{D}_1\&\mathrm{D}_2)=0$ and $D_1\&D_2=D$.

Continuing this algorithm for all statements (equations), as a result we obtain one dnf, which is the product of all statements of system (2).

Naturally, these algorithms do not always give an effect, i.e. is not universal. But if the left-hand sides of the equation are sufficiently similar d.n.f. , then the method in any case allows one to reduce the length of the products by several times.

Complexity estimates for some

a l g o r i t m o v

Let system (2) be given. In the system, consider products of the form

$$U_{1_{i_1}}\&U_{2_{i_2}}\&\ldots\&U_{m_{i_m}} \qquad (10)$$

$i_j\in\{1,2,\ldots,\mathrm{t}_j\}$.

If the product (12) is not identically zero, then applying the transformation $X_i^{\sigma_i}\&X_i^{\sigma_i}=X_i^{\sigma_i}$ in (10), we obtain the e.c. $U=X_{i_1}^{\sigma_{i_1}}\&\ldots\&X_{i_k}^{\sigma_{i_k}},\sigma_{ij}\in\{0,1\},\mathrm{j}=1,2,\ldots,\mathrm{k};\mathrm{k}\le\mathrm{n}$.

From e.c. We find solutions $\tilde{\alpha}=\left(\alpha_1,\alpha_2,\ldots,\alpha_n\right)$ of system (2). Obviously, if $U\left(\tilde{\alpha}\right)=1$, then it $\tilde{\alpha}$ is a solution to system (2).

Let us consider algorithms for solving system (2) based on the analysis of products of the type (10).

The complexity Ψ_A of algorithm A is the number of all products of the form (12) to be analyzed.

Definition. The neighborhood $S_1(U,D)$ of the first order e.c. U in d.n.f. $D = U_1 \vee U_2 \vee \ldots \vee U_m$ is the totality of all e.c. U_i from D such that $U \& U_i \neq 0$.

The number of all products of the form (2) will be denoted by Ψ. It is obvious that

$$\Psi = \prod_{i=1}^{m} t_i$$

Let D_1 be represented in a perfect d.n.f. Algorithm A_1 for solving system (2) consists in finding for each e.c. U_{1_i} $(i = 1,2,\ldots,t_1)$ such e.c. $U_{2i_2},\ldots,U_{mi_m}$, that $U_{1i} \to U_{ji_j} \equiv 1(j = 2,3,\ldots,m)$.

The solution to system (2) will be the set $\tilde{\alpha}$, where $U_{1i}(\tilde{\alpha}) = 1$.

It is easy to see that the complexity of Ψ_{A_1} Algorithm A1 satisfies the estimate

$$\Psi_{A_1} \leq 2n \cdot \sum_{i=2}^{m} t_i.$$

Obviously, $\Psi_{A_1} \leq \Psi$ if $n < \sum_{i=1}^{m} \log_2 t_i - \log\left(\sum_{i=2}^{m} t_i\right)$.

Let all statements of the system be written as derivatives of the d.n.f.

We give algorithm A2. Consider system (2).

Let $t_j = \min t_j$, $j = 1,2,\ldots,m$. For all U d.n.f. D_i we are looking for solutions to system (2) as follows:

a) we construct neighborhoods $S_1(U,D_j)$ of the first order e.c. in d.n.f. D_j, $j = 1,2,\ldots,i-1,i+1,\ldots,m$;

b) we fix the set of all vertices of $\tilde{\alpha}$ the interval U that simultaneously belong to the sets T_j of neighborhoods $S_1(U,D_j)$, $j = 1,\ldots,i-1,i+1,\ldots,m$ and, obviously, are solutions to the system (2). Here $T_j = \bigcup_{\alpha \in S_1(U,D_j)} N_\alpha$.

It is easy to see that the algorithm satisfies the estimate

$$\Psi_{A_2} \leq t_j \left(\sum_{j=1, j\neq i}^{m} t_j + |N_\alpha| \cdot \sum_{j=1, j\neq i}^{m} \left|S_1(U,D_j)\right| \right) \qquad (11)$$

where $|M|$ is the cardinality of the set M.

Based on the analysis of the neighborhood of the first order and the metric characteristics of the dnf for “almost all functions”, we can prove that the second term in (11) is asymptotically less than the first, and it suffices to calculate the order of the first term.

Hence Ψ_{A_2} in the case of reduced d.n.f. systems,etc. at $t_i = 2n \cdot n^{\log_2 \log_2 n}$ we have

$$\Psi_{A_2} \leq (m-1) n^{2\log_2 \log_2 n \ldots 22n} - \left(1+\delta(n)\right),$$

where $\delta(n) \to 0$ as $n \to \infty$.

In the case when d.n.f. system (2) is shortest, then $t_j \sim 2^{n-1} / \log_2 n$ and for Ψ_{A_2} we have

$$\Psi_{A_2} \leq (m-1) \cdot 2^{2n-2} / \log_2 2n \left(1+\delta^1(n)\right),$$ where $\delta^1(n) \to 0$ as $n \to \infty$.

CONCLUSION

In order to minimize propositions for solving systems of Boolean equations, a method is proposed for transforming propositions from the Zhegalkin polynomial into a disjunctive normal form. An algorithm for simplifying propositions in the class of disjunctive normal forms is developed. A method for multiplying propositions in the class of disjunctive normal forms is proposed. Based on the product of statements of Boolean equations, solutions of systems of Boolean equations are obtained. An estimate of the complexity of the algorithm for solving systems of Boolean equations is given.

REFERENCE

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

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

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.

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.

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.

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.

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

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

Yablonskii S.V. Vvedenie v diskretnuyumatematiku: Ucheb. posobiedlyavuzov. -2e izd., pererab. idop. -M.:Nauka. Glavnayaredaksiyafiziko-matematicheskoy literature, -384 s.

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

Leont’ev, V.K. Symmetric boolean polynomials. Comput. Math. and Math. Phys. 50, 1447–1458 (2010). https://doi.org/10.1134/S0965542510080142

Nisan, N. and Szegedy, M. (1991). On the Degree of Boolean Functions as Real Polynomials, in preparation.

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

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.

Goldberg E., Novikov Y. BerkMin: A Fast and Robust SAT Solver // Automation andTest in Europe (DATE). 2002. P. 142–149.