

МЕТОДЫ РЕШЕНИЯ СИСТЕМ НЕЛИНЕЙНЫХ БУЛЕВЫХ РАВНЕНИЙ 1-ГО ПОРЯКА

Аннотация. В статье рассматриваются методы решения систем нелинейных булевых уравнений первого порядка. Особое внимание уделено методам решения систем линейных булевых уравнений, направленным на упрощение логических высказываний. Предложен оптимальный метод решения систем линейных булевых уравнений на основе трансформации полиномов Жегалкина. Проведены исследования систем булевых уравнений произвольного базиса, а также преобразований формул в полиномиальную форму Жегалкина. Кроме того, предложен метод нахождения корней систем линейных булевых уравнений, обеспечивающий сокращение времени решения и эффективность при анализе отдельных классов систем. Результаты исследования имеют значение для оптимизации вычислительных процедур в области булевой алгебры, теории сложности и криптографического анализа.

Ключевые слова: булевы уравнения, системы нелинейных уравнений, полином Жегалкина, дизъюнктивная нормальная форма, минимизация логических функций, трансформация полиномов, методы решения.

Babadjanov Alimdjan Fazilovich

National University of Uzbekistan, Independent researcher

METHODS FOR SOLVING SYSTEMS OF FIRST-ORDER NONLINEAR BOOLEAN EQUATIONS

Abstract. The article examines methods for solving systems of first-order nonlinear Boolean equations. Special attention is given to methods for solving systems of linear Boolean equations aimed at simplifying logical expressions. An optimal method for solving systems of linear Boolean equations based on the transformation of Zhegalkin polynomials is proposed. Studies are conducted on systems of Boolean equations of arbitrary bases, as well as on the transformation of formulas into Zhegalkin polynomial form. In addition, a method for finding the

roots of systems of linear Boolean equations is proposed, which ensures reduced solution time and efficiency in analyzing specific classes of systems. The results of the study are significant for optimizing computational procedures in the fields of Boolean algebra, complexity theory, and cryptographic analysis.

Keywords: Boolean equations, systems of nonlinear equations, Zhegalkin polynomial, disjunctive normal form, minimization of logical functions, polynomial transformation, solution methods.

Babadjanov Alimdjan Fazilovich

O'zbekiston Milliy universiteti, Mustaqil izlanuvchisi

BIRINCHI DARAJALI NOCHIZIQLI BOOLEAN TENGLAMALAR TIZIMLARINI YECHISH USULLARI

Annotatsiya. Ushbu maqolada birinchi darajali nochiziqli boolean tenglamalar tizimlarini yechish usullari ko'rib chiqilgan. Maxsus e'tibor mantiqiy ifodalarni soddalashtirishga qaratilgan chiziqli boolean tenglamalar tizimlarini yechish usullariga qaratilgan. Zhegalkin polinomlarini transformatsiya qilish asosida chiziqli boolean tenglamalar tizimlarini yechishning optimal usuli taklif etilgan. Shuningdek, istalgan bazisdagi boolean tenglamalar tizimlari va formulalarni Zhegalkin polinomi shakliga aylantirish bo'yicha tadqiqotlar o'tkazilgan. Bundan tashqari, chiziqli boolean tenglamalar tizimlarining ildizlarini topish usuli taklif qilingan bo'lib, u yechim vaqtini qisqartirish va ayrim tizimlar sinflarini tahlil qilishda samaradorlikni ta'minlaydi. Tadqiqot natijalari boolean algebra, murakkablik nazariyasi va kriptografik tahlil sohalarida hisoblash jarayonlarini optimallashtirish uchun ahamiyatga ega.

Kalit so'zlar: boolean tenglamalar, nochiziqli tenglamalar tizimlari, Zhegalkin polinomi, disyunktiv normal shakl, mantiqiy funksiyalarni minimallashtirish, polinomlarni transformatsiya qilish, yechish usullari.

Введение. Пусть дана система линейных логических уравнений (л.л.у.):

$$\left. \begin{aligned} f_1 &= \sum_{j=1}^n \alpha_{1j} x_j \oplus \beta_1 = \alpha_1 \\ f_2 &= \sum_{j=1}^n \alpha_{2j} x_j \oplus \beta_2 = \alpha_2 \\ &\dots\dots\dots \\ f_m &= \sum_{j=1}^n \alpha_{mj} x_j \oplus \beta_m = \alpha_m \end{aligned} \right\} \quad (1)$$

где $\alpha_j, \beta_j, \alpha_{ij} \in \{1,0\}, i=1, \dots, m; j=1, \dots, n$. Здесь символ $\oplus$ подразумевается кратным логическим сложением по модулю 2.

Известно, что система л.л.у. (1) может не иметь общего решения, т.е. уравнения несовместны. Поэтому прежде всего необходимо определить совместность всех уравнений системы и при наличии несовместных уравнений исключить из системы, а затем перейти к ее решению.

Пусть $f_{i_1}(x_1, \dots, x_n) = \alpha_{i_1}$ и $f_{i_2}(x_1, \dots, x_n) = \alpha_{i_2}$ л.л.у. системы (1). Ясно, что уравнения $f_{i_1}(x_1, \dots, x_n) = \alpha_{i_1}$ и $f_{i_2}(x_1, \dots, x_n) = \alpha_{i_2}$ будут несовместными, если $f_{i_1} \oplus f_{i_2} = \text{const} = \alpha$ и $\alpha_{i_1} \oplus \alpha_{i_2} \neq \alpha; \alpha_{i_1}, \alpha_{i_2}, \alpha \in \{0,1\}$. В случае, когда $\alpha_{i_1} \oplus \alpha_{i_2} = \alpha$, уравнения называются эквивалентными.

Задачу удаления несовместных уравнений будем выполнять применением методов сложения по модулю 2 и последовательным исключением переменных.

Пусть система (2.1) приведена методом исключения переменных к виду

$$\left. \begin{aligned} \sum_{j=1}^n a_{1j} x_j \oplus \beta_1 &= \alpha_1 \\ \sum_{j=2}^n a'_{2j} x_j \oplus \beta_2 &= \alpha'_2 \\ &\dots\dots\dots \\ \sum_{j=1}^n a'_{mj} x_j \oplus \beta_m &= \alpha'_m \end{aligned} \right\} \quad (2)$$

Проверяем для уравнений $f_2, f_3, \dots, f_m$ условия равенства: $f_i = f_j; i, j = 2, 3, \dots, m; i \neq j$. Положим, что $f_{i_1} = f_{i_2} = \dots = f_{i_k}, \{i_1, \dots, i_k\} \in \{2, \dots, m\}$.

Тогда возможно два случая:

- а) $\alpha_{i_1} = \alpha_{i_2} = \dots = \alpha_{i_k}$,
- б) $\alpha_{i_1} = \alpha_{i_2} = \dots = \alpha_{i_k} = \bar{\alpha}_{i_{k+1}} = \dots = \bar{\alpha}_{i_{k+t}} \cdot 1 + t = k$.

Очевидно, что в случае а) уравнения $f_{i_1} \overset{\text{б}}{\sim} \alpha_{i_1}, \dots, f_{i_k} \overset{\text{б}}{\sim} \alpha_{i_k}$ эквивалентны, так как $\bar{\alpha}_{i_{k+1}} = \dots = \bar{\alpha}_{i_{k+t}}, f_{i_1} \oplus f_{i_t} = \text{const} = \alpha, \alpha_{i_1} \oplus \alpha_{i_t} = \alpha, \alpha \in \{0,1\}$ и в системе (2) достаточно оставить одно из уравнений $f_{i_1} \overset{\text{б}}{\sim} \alpha_{i_1}, \dots, f_{i_k} \overset{\text{б}}{\sim} \alpha_{i_k}$. В случае б) имеются

одновременно эквивалентные и несовместные уравнения, т.е.

$$f_{i_j} \oplus f_{i_t} = \text{const} = \alpha; j, t = 1, \dots, k; \alpha_{i_j} \oplus \alpha_{i_t} \neq \alpha, j = 1, 2, \dots, t; t = l+1, l+2, \dots, l+n; \alpha_{i_j} \oplus \alpha_{i_t} = \alpha, j, t = l+1, l+2, \dots, l+n$$

Поэтому здесь исключаем группы с меньшим количеством уравнений.

Пусть $n < l$. Тогда уравнения $f_{i_{n+1}} \dot{\alpha}_{i_{n+1}}, \dots, f_{i_{l+n}} \dot{\alpha}_{i_{l+n}}$ исключаем из системы, так как они несовместны. Затем, как в первом случае, в системе оставим одно из эквивалентных уравнений $f_{i_1} \dot{\alpha}_{i_1}, \dots, f_{i_l} \dot{\alpha}_{i_l}$ например $f_{i_1} \dot{\alpha}_{i_1}$.

Теперь фиксируем второе уравнение полученной системы и применяется метод исключения переменных (для переменной x_2) для остальных уравнений, кроме первого и второго, снова применяя алгоритм нахождения несовместных уравнений и т.д.

Процесс продолжается до тех пор, пока не будут просмотрены все уравнения в системе и не будет получена совместная подсистема системы (2.1) в виде

$$\left\{ \begin{array}{l} \sum_{j=1}^n a_{1j} x_j \oplus \beta_1 = \alpha_1 \\ \sum_{j=i_1}^n a_{2j}^1 x_j \oplus \beta_2^1 = \alpha_2^1 \\ \dots \\ \sum_{j=i_k}^n a_{k+1,j}^k x_j \oplus \beta_{k+1}^k = \alpha_{k+1}^k \end{array} \right. \quad (3)$$

где $1 < i_1 < \dots < i_k; k+1 \leq m; \beta_1, \beta_l^{l-1} \beta_l - 1, \alpha_1, \square_l^{l-1} \in \{0, 1\}; l=1, 2, \dots, k;$

$\square_{ij}^l \in [0,1]; i=1,...,k+1; j=1,2,...,n$ в которой $k+1 \leq n$, где n - число переменных.

Если система (1) не имеет совместных и эквивалентных уравнений, тогда легко увидеть, что система (3) имеет $k+1=m$ уравнений и он является эквивалентной системе (1).

Решении и их оценки. Пусть система(2.1) совместна и приведена к виду (3), в котором $k+1=m$. Положим NN -количество решений системы(1) .

Теорема-1. $NN=2^{n-m}$, где n —число переменных, m —количество уравнений.

Доказательство: Система (1) легко приводится к эквивалентному виду:

$$\left\{ \begin{array}{l} \sum_{i=i_1}^n a_{1i}^0 x_i \oplus b_1^{0,0} \mathbf{e}_{\square} \\ \dots\dots\dots \\ \sum_{i=i_m}^n a_{mi}^{m-1} x_i \oplus b_m^{m-1} \mathbf{e}_m^{(m-1)} \end{array} \right. \quad (4)$$

где $\square_i^j, b_i^j, a_{ij}^l \in [0, 1]; i=1, \dots, m; j=0, \dots, m-1; l=i_1, \dots, n; i_1=1, i_1 < i_2 < \dots < i_m$.

Теперь последнее уравнение

$$\sum_{i=i_m}^n \alpha_{mi}^{m-1} x_i \oplus b_m^{m-1} = \alpha_m^{m-1}$$

приведем к виду

$$\sum_{i=i_m}^n a_{mi}^{m-1} x_i = \alpha_m^m \quad (5)$$

$$\text{где } \alpha_m^m = \begin{cases} \alpha_m^{m-1}, & \text{если } b_m^{m-1} = 0, \\ \bar{\alpha}^{m-1}_m - \text{в противном случае} \end{cases}$$

Пусть l – число участвующих переменных, t – число не участвующих переменных, начиная с x_{i_m} в уравнении (5). Здесь $t = n - i_m - l + 1 = n - (i_m + l - 1)$

Известно, что высказывание $\sum_{i=1}^m A_i$ преобразуется в д.н.ф. с помощью известных тождеств

$$\left[A_j \right]_v^m = A_1^{\sigma_1} \wedge A_2^{\sigma_2} \wedge \dots \wedge A_m^{\sigma_m}, \quad \text{где } (\sigma_1 \oplus \dots \oplus \sigma_m) = 1, (\sigma_1, \sigma_2, \dots, \sigma_m) \in E^m \text{ и содержит } 2^{m-1} \text{ элементарных конъюнкции, соответствующих решению уравнений}$$

$$\sum_{i=1}^m A_i = \alpha, \alpha \in [0, 1].$$

Следовательно, число решений R_y для участвующих переменных уравнения (5) равно 2^{l-1} и число решений для не участвующих переменных после переменной x_{i_m} соответствует всевозможному набору t элементов, т.е.

$$R_H = 2^t = 2^{n - (i_m + l - 1)}$$

Тогда количество решений уравнения (5) для переменных $x_{i_m}, \dots, x_n$ равно $R = R_y \cdot R_H = 2^{l-1} \cdot 2^{n - i_m - l + 1}$.

Пусть $\tilde{\alpha}_{i_{m_1}}, \tilde{\alpha}_{i_{m_2}}, \dots, \tilde{\alpha}_{i_{m_l}}$ корни уравнения (5) для переменных $x_{i_m}, \dots, x_n$.

Рассмотрим решение для переменных $x_1, \dots, x_{i_{m-1}}$. Нетрудно заметить, что если в (2.4) $m = i_m$, т.е. $i_1 = 1, i_2 = 2, \dots, i_{m-1} = m - 1$, то при операции обратного перехода для каждого уравнения (5) остальным переменным соответствует только одно решение и система (2.4) имеет

$$NN = 2^{n - i_m} = 2^{n - m}$$

решений.

Предположим, что $m < i_m$. Нетрудно заметить, что при нахождении корней с помощью метода обратного перехода (для переменных $x_1, \dots, x_{i_{m-1}}$) в каждом промежутке $(i_{m-k}, i_{m-k+1}; k = 1, \dots, m-1)$ решение $(\tilde{\alpha}_{i_{m_1}}, \tilde{\alpha}_{i_{m_2}}, \dots, \tilde{\alpha}_{i_{m_l}})$ увеличивается в $2^{(i_{m-k+1}-1) - i_{m-k}}$ раз за счет добавления корней переменных $x_{i_{m-k}}, x_{i_{m-k}+1}, \dots, x_{i_{m-k+l}+l}$. Следовательно, для уравнений имеем

$$NN = 2^{n-i_m} \cdot 2^{i_m-1-i_{m-1}} \cdot 2^{i_{m-1}-1-i_{m-2}} \cdot \dots \cdot 2^{i_2-1-i_1}$$

решений. Учитывая, что $i_1=1$ и m -число сомножителей, после несложных преобразований имеем $NN=2^{n-m}$.

Теорема доказана.

Нетрудно заметить, что если $n=m$, то система имеет единственное решение, т.е. $NN=2^{n-m}=2^0=1$.

Следствие-1. Любая произвольная система линейных логических уравнений имеет не более 2^{n-1} решений, где n - число переменных.

Методы трансформации. Рассматриваем аналитические критерии преобразования, исследующие вопросы преобразования формул над произвольным базисом $\{\neg x, x_1 \wedge x_2, x_1 \vee x_2, x_1 \rightarrow x_2, x_1 \oplus x_2, x_1 \rightarrow x_2, x_1 / x_2\}$ в формулы над базисом: $\{0, 1, x_1 \wedge x_2, x_1 \oplus x_2\}$.

Здесь рассматривается критерий преобразования формул:

$$\{U_i\}^m \equiv \{U_j\}_{\Sigma}^{m^1}, \{U_i\}_{\vee}^m \equiv \{U_j\}_{\Sigma}^{m^1}, \{U_i\}_{\rightarrow}^m \equiv \{U_j\}_{\Sigma}^{m^1}, \{U_i\}_I^m \equiv \{U_j\}_{\Sigma}^{m^1}$$

(что позволяет исключить промежуточные результаты в процессе преобразования) и оценка их сложности – $K_{o_2}^{o_1}(m), L_{o_2}^{o_1}(m)$, а так же рассмотрен и теоретически обоснован новый подход к преобразованию формул над произвольным базисом к полиному Жегалкина.

Теорема-2. Преобразование $\{U_j\}_{\vee}^m \equiv \{U_j\}_{\Sigma}^{m^1}$ имеет вид

$$\{U_j\}_{\Sigma}^{m^1} = \sum \left(U_{i_1}^{\sigma_{i_1}} \wedge U_{i_2}^{\sigma_{i_2}} \wedge \dots \wedge U_{i_k}^{\sigma_{i_k}} \right), \quad (6)$$

где

$$(\sigma_1 \vee \sigma_2 \vee \dots \vee \sigma_m = 1), \{\sigma_{i_1}, \sigma_{i_2}, \dots, \sigma_{i_k}\} \in \{\sigma_1, \sigma_2, \dots, \sigma_m\}, \sigma_{i_1} = \sigma_{i_2} = \dots = \sigma_{i_k} = 1, i_k \in \{1, 2, \dots, m\}, k \leq m$$

.

и

$$L_{\Sigma}^{\vee}(m) = \sum_{i=1}^m (i \cdot C_m^i), K_{\Sigma}^{\vee}(m) = 2^m - 1$$

Доказательство. Через B_k и l_k обозначим выражение и число с.к. после преобразования формул $i=1 \dots k B_k$ полиному Жегалкина.

Для $k=2$ и $k=3$ формулы находим очень просто:

$$\begin{aligned} U_1 \vee U_2 &= U_1 U_2 \oplus U_1 \oplus U_2 = B_2, l_2 = 3; \\ U_1 \vee U_2 \vee U_3 &= B_2 U_3 \oplus B_2 \oplus U_3 = U_1 U_2 U_3 \oplus U_1 U_3 \oplus \\ &\oplus U_2 U_3 \oplus U_1 U_2 \oplus U_1 \oplus U_2 \oplus U_3 = B_3, l_3 = l_2 + l_2 + 1 = 7. \end{aligned}$$

Пусть $k=n+1$, тогда справедливо следующее:

$$U_1 \vee U_2 \vee \dots \vee U_n \vee U_{n+1} = B_n U_{n+1} \oplus B_n \oplus U_{n+1}, l_{n+1} = 2l_n + 1.$$

Если для $B_k (k=1, \dots, n+1)$ число с.к. вычисляем последовательно:

$$k=1, l_1=1=2^1-1, k=2, l_2=2l_1+1=3=2^2-1, k=3, l_3=2l_2+1=7=2^3-1,$$

$$\dots\dots\dots k=n+1, l_{n+1}=2l_n+1=2^{n+1}-1,$$

то нетрудно заметить, что для m переменных имеем

$$l_m = K_{\Sigma}^{\vee}(m) = 2^m - 1.$$

Если учесть, что $E_m^2 = 2^m$ и $K_{\Sigma}^{\vee}(m) = 2^m - 1$, то разложение состоит из всевозможных единичных m -мерных кубов, через которые можно легко записать в аналитическом виде формулу (2.8). Известно, что в каждом уровне $\mathfrak{Z}$ -мерного куба имеется C_m^i наборов и в каждом наборе участвует i единиц, которым соответствует m переменных. Следовательно, вхождение переменных в полином $(U_j)_{\Sigma}^{i, m, 1}$ равно

$$L_{\Sigma}^{\vee}(m) = \sum_{i=1}^m (i \cdot C_m^i).$$

Теорема доказана.

Заключение

Исследована система булевых уравнений произвольного базиса и преобразование формул над произвольном базисом в формулы полинома Жегалкина. Разработан метод преобразования высказываний системы на специальные дизъюнктивные нормальные формы и методы умножения сложных конъюнкции. Разработан метод нахождения корней систем линейных булевых уравнений первого порядка на основе трансформации полиномов.

Список использованной литературы

1. Байжуманов А.А. Эффективное использование линейных форм при решении систем логических уравнений второй степени. // Сборник материалов международной научной конференции «Наука и инновации: новости, проблемы и достижения», 30-31 мая 2022, Туркестан, 2022. – С. 169–173.
2. Кабулов А.В., Байжуманов А., Бердымуродов М.А. Methods for minimizing disjunctions of systems of nonlinear Boolean equations, based on information about the neighborhood of the 1st order (Методы минимизации

дизъюнктивных нормальных форм систем нелинейных булевых уравнений, основанные на информации об окрестностях 1-го порядка) // Республиканская научно-техническая конференция «Современное состояние и перспективы развития цифровых технологий и искусственного интеллекта», Самарканд, 26-27 октября 2022. – С. 37–43.

3. Кабулов А., Норматов И., Урунбаев Э., Мухаммадиев Ф. Инвариантное продолжение дискретных многозначных функций и их реализация. – 2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), 2021. doi:10.1109/IEMTRONICS52119.2021.9422486

4. Бабаджанов А., Сайманов И. Алгебраические методы решения задач распознавания с непересекающимися классами. – 2022 Международная конференция по информатике и коммуникационным технологиям (ICISCT), 2022. – С. 1–5.