

Норматов Иброхимали Холмаматович

Профессор Национального университета Узбекистана имени М.Улугбека

i_normatov@nuu.uz

Бабаджанов Алимджан Фазылович

Старший научный сотрудник Инженерной федерации Узбекистана

Кудайбергенов Адилбай

Докторант Национального университета Узбекистана имени М.Улугбека

ИССЛЕДОВАНИЕ МЕТОДОВ ПОИСКА МАКСИМАЛЬНЫХ СОВМЕСТНЫХ ПОДСИСТЕМ СИСТЕМ НЕЛИНЕЙНЫХ БУЛЕВЫХ УРАВНЕНИЙ

Аннотация. В статье представлена задача поиска решений систем булевых уравнений с целью повышения точности эвристических методов решения практических задач алгебраического криптоанализа, прогнозирования, распознавания, классификации и поиска абсолютных экстремумов множества переменных. Также путем решения задачи декодирования и нахождения максимального верхнего нуля монотонных логических функций был разработан алгоритм поиска максимальных подсистем систем логических уравнений.

Ключевые слова: алгоритм, эвристический метод, булевых уравнений, абсолютный экстремум, декодирования, монотонная логическая функция, система.

Normatov Ibrokhimali Kholmatovich

Professor of the National University of Uzbekistan named after M. Ulugbek

i_normatov@nuu.uz

Babajanov Alimdzhon Fazilovich

Senior Researcher at the Engineering Federation of Uzbekistan

Kudaibergenov Adilbay

Doctoral student at the National University of Uzbekistan

RESEARCH OF METHODS FOR SEARCHING MAXIMUM COMPATIBLE SUBSYSTEMS OF SYSTEMS OF NONLINEAR BOOLEAN EQUATIONS

Annotation. The article presents the problem of finding solutions to systems of Boolean equations in order to increase the accuracy of heuristic methods for solving practical problems of algebraic cryptanalysis, forecasting, recognition, classification and search for absolute extrema of many variables. Also, by solving the problem of decoding and finding the maximum upper zero of monotonic logical functions, an algorithm for searching for maximum subsystems of systems of logical equations was developed.

Key words: algorithm, heuristic method, Boolean equations, absolute extremum, decoding, monotonic logical function, system.

Normatov Ibroximali Xolmatovich

M.Ulug'bek nomidagi O'zbekiston Milliy universiteti professori

i_normatov@nuu.uz

Babajanov Alimdjan Fazilovich
O'zbekiston muhandislar federatsiyasi katta ilmiy xodimi
Xudoybergenov Adilbay
M.Ulug'bek nomidagi O'zbekiston Milliy universiteti doktoranti

NOCHIZIQLIY BUL TENGLAMALAR TIZIMLARINING MAKSIMAL O'ZARO QISIM TIZIMLARINI IZLASH USULLARINI TADQIQOTI

Annotatsiya. Maqolada algebraik kriptotahlil, prognozlash, tanib olish, tasniflash va ko'p o'zgaruvchilarning mutlaq ekstremallarini qidirishning amaliy masalalarini yechishning evristik usullarining aniqligini oshirish uchun Bul tenglamalari tizimlarining echimlarini topish muammosi keltirilgan bo'lib, nochiziqli mantiqiy tenglamalar tizimlarining maksimal izchil quyi tizimlarini izlash usullarini o'rganish amalga oshirilgan. Shuningdek dekodlash va monotonik mantiqiy funktsiyalarning maksimal yuqori nolini izlash masalasini hal qilish orqali mantiqiy tenglamalar tizimlarining maksimal quyi tizimlarini izlash algoritmi ishlab chiqilgan.

Kalit so'zlar: algoritm, evristik usul, mantiqiy tenglamalar, absolyut ekstremum, dekodlash, monoton mantiqiy funktsiya, tizim.

Введение

В настоящее время в мире особое внимание уделяется использованию информационных технологий в различных отраслях, в особенности в сфере применения их в государственном управлении и системе самоуправления, актуальной проблемой является применение технологий и методов обеспечения корректности информации в цифровой экономике, при предоставлении физическим и юридическим лицам различных государственных интерактивных услуг, расширения возможностей интеграции хозяйственных систем в мировом масштабе. Поэтому для обеспечения выполнения постановления особое значение приобретает проблема поиска решений систем булевых уравнений для повышения точности эвристических методов решения прикладных задач алгебраического криптоанализа, прогнозирования, распознавания, классификации, поиска абсолютных экстремумов функций многих переменных [1-5].

1. Об одном алгоритме поиска максимального верхнего нуля монотонных булевых функций.

Пусть E_n^2 - n - мерный двочный куб. Нормой $|\tilde{\alpha}|$ набора $\tilde{\alpha}$ в E_n^2

назовем число единичных элементов. Число $A_{\tilde{\alpha}} = \sum_{i=1}^n \alpha_i \cdot 2^{n-i}$ будем называть номером $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Будем говорить, что наборы $\tilde{\alpha}$ k -го уровня упорядочены в лексикографическом порядке, если они расположены в порядке убывания наборов $A_{\tilde{\alpha}}$.

Считаем, что набор $\tilde{\beta}$ непосредственно следует за $\tilde{\alpha}$ на k -м уровне, $k = \overline{1, n}$, если $A_{\tilde{\beta}} < A_{\tilde{\alpha}}$ и не существует такого $\tilde{\gamma}$, где $|\tilde{\gamma}| = k$, что $A_{\tilde{\beta}} < A_{\tilde{\gamma}} < A_{\tilde{\alpha}}$.

Определение-1. Функция $f(x_1, x_2, \dots, x_n)$ называется монотонной, если для любых двух наборов $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$ таких, что $\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \dots, \alpha_n \leq \beta_n$ имеет место неравенство $f(\tilde{\alpha}) \leq f(\tilde{\beta})$.

Пусть M_n – множество всех монотонных булевых функций от n переменных. Набор $\tilde{\alpha} \in E_n^2$ назовем верхним нулем функции $q \in M_n$, если $q(\tilde{\alpha}) = 0$ и для любого набора $\tilde{\beta} \in E_n^2$, $|\tilde{\alpha}| \leq |\tilde{\beta}|$ следует, что $q(\tilde{\beta}) \neq 0$.

Верхний нуль $\tilde{\alpha}$ функции $q \in M_n$ называется ее максимальным верхним нулем (м.в.н.), если для верхнего нуля $\tilde{\beta}$ функции q будет $|\tilde{\beta}| \leq |\tilde{\alpha}|$.

Пусть произвольная функция $q \in M_n$ задана при помощи оператора A_q , который по любому набору $\tilde{\alpha} \in E_n^2$ выдает значение $q(\tilde{\alpha})$. Задача поиска м.в.н. функций из M_n - формируется следующим образом. Если некоторая функция $q \in M_n$ задана оператором A_q , то требуется минимальным числом обращений к A_q найти хотя бы один м.в.н. функции $q(x_1, x_2, \dots, x_n)$.

Опишем алгоритм A_M , где используется лексикографический порядок расположение наборов уравнений E_n^2 .

Алгоритм A_M состоит из двух этапов:

Этап I. На первом шаге алгоритма вычисляем значение q на наборе $\tilde{\alpha}_1$ с наибольшим номером $\left\lfloor \frac{n}{2} \right\rfloor$ -го уровня.

Пусть на i -м шаге вычислено значение q на некотором наборе $\tilde{\alpha}_i$ $\left\lfloor \frac{n}{2} \right\rfloor - i + 1$ -го уровня, $1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor$. Если $q(\tilde{\alpha}_i) = 1$, то на $(i+1)$ -м шаге вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ с наибольшим номером $\left\lfloor \frac{n}{2} \right\rfloor - i$ -го уровня. Если же $q(\tilde{\alpha}_i) = 0$, то переходим по второму этапу алгоритма. Если на $\left\lfloor \frac{n}{2} \right\rfloor + 1$ -м шаге получено $q\left(\alpha_{\left\lfloor \frac{n}{2} \right\rfloor + 1}\right) = 1$, то $q = 1$ и алгоритм заканчивает работу.

Этап II. Пусть к началу второго этапа алгоритма сделано $\tau + 1$ шагов $\left(0 \leq \tau \leq \left\lfloor \frac{n}{2} \right\rfloor\right)$, т.е. вычислены значения $q(\tilde{\alpha}_1) = q(\tilde{\alpha}_2) = \dots = q(\tilde{\alpha}_\tau) = 1$ и $q(\tilde{\alpha}_{\tau+1}) = 0$, где $\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_{\tau+1}$ – с наибольшими номерами $\left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor - 1, \dots, \left\lfloor \frac{n}{2} \right\rfloor - \tau$ уровней соответственно. Тогда на $(\tau + 2)$ -м шаге вычисляем значение q на наборе $\tilde{\alpha}_{\tau+2}$ $\left\lfloor \frac{n}{2} \right\rfloor - \tau + 1$ -го уровня, непосредственно следующем за $\tilde{\alpha}_\tau$ в лексикографическом порядке, на котором значение q еще не определено. Причем, если $\tau = 0$, то за $\tilde{\alpha}_{\tau+2}$ берем крайний левый набор уровня $\left\lfloor \frac{n}{2} \right\rfloor - i + 1$.

Пусть на i -м шаге ($i \geq \tau + 2$) вычислено значение q на некотором наборе $\tilde{\alpha}_i$ j -го уровня, где $j \geq \left\lfloor \frac{n}{2} \right\rfloor - \tau + 1$. Если $q(\tilde{\alpha}_i) = 1$, то на $(i+1)$ -м шаге

вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ того же j -го уровня, непосредственно следующем в лексикографическом порядке за $\tilde{\alpha}_i$. Если такого набора не существует, то алгоритм заканчивает работу. Если же $q(\tilde{\alpha}_i)=0$, то на $(i+1)$ -м шаге вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ $(j+1)$ -го уровня, непосредственно следующем в лексикографическом порядке за набором $\tilde{\alpha}$ с наименованием номеров $(j+1)$ -го уровня таким, что $q(\tilde{\alpha})$ определена непосредственно или по монотонности и $q(\tilde{\alpha})=1$. Причем, если набор $\tilde{\alpha}$ не существует, то за $\tilde{\alpha}_{i+1}$ берем набор с наибольшим номером $(j+1)$ -го уровня. В случае, когда не существует набор $\tilde{\alpha}_{i+1}$, удовлетворяющий указанным свойствам, алгоритм останавливается.

Пусть алгоритм сделал r шагов до остановки. Получаем цепочку наборов $\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_r$, на которых последовательно вычислялось значение q . Тогда м.в.н. функции q – это такой набор $\tilde{\alpha}_s$ на этой цепочки с максимальным s , что $q(\tilde{\alpha}_s)=0$. Действительно, из описания алгоритма следует, что на всех наборах $|\tilde{\alpha}_s|+1$ -го уровня функции q определена по монотонности или непосредственно и равна единице [2-3].

2. Решение задачи поиска максимальных совместных подсистем.

Пусть дана система булевых уравнений:

$$M = \begin{cases} f_1(x_1, x_2, \dots, x_n) = 1 \\ f_2(x_1, x_2, \dots, x_n) = 1 \\ \dots\dots\dots \\ f_m(x_1, x_2, \dots, x_n) = 1 \end{cases} \quad (1)$$

Определение-2. Весом P_i уравнения $f_i, i = \overline{1, m}$ назовем число всех $f_i \in M$ таких, что $f_i \cdot f_j \neq 0, i \neq j$.

Пусть $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}$ суть единичные координаты набора $\tilde{\alpha} = (\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_m) \in E_m^2$.

Рассмотрим монотонную булеву функцию $q(y_1, y_2, \dots, y_m)$:

$$q(y_1, y_2, \dots, y_m) = \begin{cases} 0, & \text{если } \{f_{i_1} = 1, f_{i_2} = 1, \dots, f_{i_k} = 1\} \text{ совместна,} \\ 1 & \text{в противном случае.} \end{cases}$$

Для нахождения максимальной совместной подсистемы системы (1) применяем алгоритм A_M поиска максимального верхнего нуля (м.в.н.) функции $q(y_1, y_2, \dots, y_m)$. Причем поиск м.в.н. функции $q(\tilde{y})$ ведется в лексикографическом порядке наборов переменных $y_{i_1}, y_{i_2}, \dots, y_{i_m}$, для которых $P_{i_1} \geq P_{i_2} \geq \dots \geq P_{i_m}$. На каждом шаге обращение к оператору O_q для вычисления значений $q(\alpha_1, \alpha_2, \dots, \alpha_m)$ на наборе $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_m)$, у которого $\square_{i_1}, \dots, \square_{i_k}$ суть единичные координаты, используем процедуру распознавания совместности подсистемы $\{f_{i_1} = 1, f_{i_2} = 1, \dots, f_{i_k} = 1\}$ системы (1).

Исследуем процесс вычисления значений $q(y_1, y_2, \dots, y_m)$ на наборе E_n^2 .

Пусть

$$\begin{cases} f_{i_1}(x_1, x_2, \dots, x_n) = 1 \\ f_{i_2}(x_1, x_2, \dots, x_n) = 1 \\ \dots\dots\dots \\ f_{i_t}(x_1, x_2, \dots, x_n) = 1 \end{cases} \quad (2)$$

подсистема системы (1).

Рассмотрим матрицу $\|a_{ij}\|_{t \times t}$:

$$a_{ij} = \begin{cases} 1, & \text{если } f_{i_j} \cdot f_{i_i} \neq 0, i, j = \overline{1, t}; \\ 0 & \text{в противном случае.} \end{cases}$$

Очевидно, что матрица $\|a_{ij}\|_{t \times t}$ симметрична и, если система (2) совместна, то $f_{i_i} \cdot f_{i_j} \neq 0, i, j = \overline{1, t}$, и соответственно, в этом случае $\|a_{ij}\|_{t \times t}$ - однородно-единичная матрица. В дальнейшем мы будем так называть те матрицы, все элементы которой равны единице. Если в матрице $\|a_{ij}\|_{t \times t}$ имеется хотя бы один элемент $a_{ij} = 0$, система несовместна.

Положим, что высказывания $f_i, i = \overline{1, m}$ системы (1) заданы в базисе: $\{\bar{X}, x_1 \wedge x_2, x_1 \vee x_2\}$.

Пусть подсистема (2) имеет вид:

$$\begin{cases} U_{11} \vee U_{12} \vee \dots \vee U_{1p_1} = 1 \\ U_{21} \vee U_{22} \vee \dots \vee U_{2p_2} = 1 \\ \dots\dots\dots \\ U_{t1} \vee U_{t2} \vee \dots \vee U_{tp_t} = 1 \end{cases} \quad (3)$$

Определим условия совместности системы (3). Нетрудно заметить, что система (3) совместна в том и только в том случае, если существует э.к.

$U_{1j_1}, U_{2j_2}, \dots, U_{tj_t}$, такие что

$$\bigwedge_{k=1}^t U_{kj_k} \neq 0. \quad (4)$$

Предлагаем одну из эффективных процедур проверки (ПП) выполнения условия (4). Представим д.н.ф. $N_i, i = \overline{1, t}$ системы (3) в ортогональной д.н.ф. $N_i^0 = K_{i1} \vee K_{i2} \vee \dots \vee K_{it_i}$. Индукцией по $i, (i = \overline{1, t-1})$ определяем совместность системы.

1-шаг индукции. Для э.к. $K_{1j}, j = \overline{1, t_1}$ д.н.ф. N_1^0 фиксируем э.к. $K_{21}, K_{22}, \dots, K_{2k}$ в д.н.ф. N_2^0 такие, что $K_{2i} \cdot K_{1j} \neq 0, i = \overline{1, k}$.

Пусть $\tilde{T}_j = \{\mathfrak{T}_1, \mathfrak{T}_2, \dots, \mathfrak{T}_k\}$, где $\mathfrak{T}_i = K_{2i} \cdot K_{1j} \neq 0$, $i = \overline{1, k}$. Причем, если очередного K_{2i} имеет место $K_{1j} \rightarrow K_{2i} = 1$, то $\tilde{T}_j = \{\mathfrak{T}_1\}$, где $\mathfrak{T}_1 = K_{1j} \cdot K_{2i} = K_{1j}$.

Положим $T_1 = \bigvee_{j=1}^{t_1} \tilde{T}_j$. В случае, когда $T_1 = 0$, алгоритм заканчивает свою работу, и система (3) несовместна.

Пусть на $(i - 1)$ -м шаге построено множество T_{i-1} э.к.

i-й шаг индукции. Для всех э.к. U из T_{i-1} формируем множество $T_{\mathfrak{T}}$ э.к. $\mathfrak{T} = U \cdot B$, где B э.к. в д.н.ф. N_{i+1}^0 и $U \cdot B \neq 0$.

Пусть множество $T_i = \bigvee_{\mathfrak{T}: \mathfrak{T} \in T_{i-1}} T_{\mathfrak{T}}$. Если $T_i = 0$, то алгоритм заканчивает свою работу и система (3) несовместна.

Положим, что после $(t-1)$ – го шага индукции построено множество T_{t-1} э.к. такое, что $T_{t-1} \neq 0$. Отсюда следует, что система (3) совместна.

Таким образом, общий алгоритм определения совместности подсистемы (2) системы (1), заданной в виде (3), состоит из двух этапов. На первом этапе строим однородно-единичную матрицу $\|a_{ij}\|_{t \times t}$ и переходим ко второму этапу. На втором этапе к системе (3) применяем процедуру ПП.

Приближенный алгоритм поиска.

Пусть $M = \{f_1 = 1, f_2 = 1, \dots, f_m = 1\}$,

$$a_{ij} = \begin{cases} 1, & \text{если } f_i \cdot f_j \neq 0, i, j = \overline{1, m}; \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть $A_{i_1 i_2 \dots i_k}$ – квадратная подматрица матрицы $A = \|a_{ij}\|_{m \times m}$, составленная из элементов a_{ij} , где $i, j = i_1, i_2, \dots, i_k$, $1 \leq k \leq m$.

Подматрицу $A_{i_1 i_2 \dots i_k}$ не содержащую нулей, назовем максимальной, если любая другая квадратная подматрица, включающая в себя $A_{i_1 i_2 \dots i_k}$, не является однородно-единичной матрицей.

Считается, что $A_{i_1 i_2 \dots i_k}$ соответствует подмножеству $\{f_{i_1}=1, f_{i_2}=1, \dots, f_{i_k}=1\}$ на M и задается монотонной функцией $q(y_{i_1}, y_{i_2}, \dots, y_{i_k})$.

Алгоритм поиска максимальных совместных подсистем состоит в следующем:

Этап I. Находим все однородно – единичные подматрицы матрицы $\|a_{ij}\|$.

Этап II. Для всех максимальных подматриц $A_{i_1 i_2 \dots i_k}$ строим систему $M_{i_1 i_2 \dots i_k} = \{f_{i_1}=1, f_{i_2}=1, \dots, f_{i_k}=1\}$ и, применяя алгоритм A_M , находим м.в.н. монотонной булевой функции, соответствующей $M_{i_1 i_2 \dots i_k}$.

Обозначим через $\{A\}$ множество всех максимальных однородно-единичных подматриц в $\|a_{ij}\|$.

Пусть $A_{i_1 i_2 \dots i_k}$ – максимальная подматрица из $\{A\}$ и $q(y_{i_1}, y_{i_2}, \dots, y_{i_k})$ – монотонная булева функция, соответствующая подсистеме $M_{i_1 i_2 \dots i_k}$. Множество всех таких булевых функции обозначим через $\tilde{A}$.

Пусть $|\tilde{\alpha}| = \left(\begin{array}{c} \max |\tilde{\beta}| \\ \tilde{\beta} \text{ м.в.н. } q \in \tilde{A} \end{array} \right)$. Очевидно, что $\tilde{\alpha}$ есть м.в.н. $q(y_1, y_2, \dots, y_m)$.

Таким образом, задача поиска м.в.н. $q(y_1, y_2, \dots, y_m)$ свелась к нахождению м.в.н. всех монотонных булевых функции из $\tilde{A}$.

Приближенный алгоритм строим в два этапа. На первом этапе строим максимальную подматрицу $A_{i_1 i_2 \dots i_k}$ так, что $k = \left(\begin{array}{c} \max t \\ A_{i_1 i_2 \dots i_t} \in \{A\} \end{array} \right)$.

На втором этапе, применяя алгоритм A_M , ищем м.в.н. $q(y_{i_1}, y_{i_2}, \dots, y_{i_k})$. Для этого на первом этапе из A удаляем нулевые строки и столбцы с наименьшей нормой. Первый этап состоит из двух подэтапов. На первом выявляется i -я строка и i -й столбец с наименьшим числом единиц. На втором из A удаляем i -ю строку и i -й столбец. Если $A_{i_1 i_2 \dots i_k}$ - единичная матрица, то алгоритм заканчивает свою работу. В противном случае возвращаемся к первому подэтапу.

Заключение

Проведено исследование методов поиска максимальных совместных подсистем систем нелинейных булевых уравнений. Разработан алгоритм поиска максимальных подсистем систем булевых уравнений на основе решения задачи расшифровки и поиска максимального верхнего нуля монотонных булевых функций.

Литература

1. Бусленко В.Н., Каганович В.Л., Дашкова В.Г. Вопросы разработки технологии агрегативного моделирования- Программирование, 1988, №1, С. 66-76.
2. Кабулов В.К., Кабулов А.В., Норматов И.Х. Алгоритмизация в теории управляющих систем//Монография: Ташкент-2017, Изд. “Навруз” С.176.
3. Кабулов В.К., Кабулов А.В., Норматов И.Х. Логические методы алгоритмизации в теории управляющих систем. Монография: Германия.2018, Изд. “Ламберт” С.191.
4. Скляр В.А., Кабулов А.В. Микропроцессорная система с распределенным управлением// ДАН УзССР, 1988, № 7, С.12-14.
5. Кабулов А., Норматов И.Х. и др, Инвариантное продолжение дискретных многозначных функций и их реализация.–2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021. – С. 1 -6, doi: 10.1109/IEMTRONICS52119.2021.9422486.