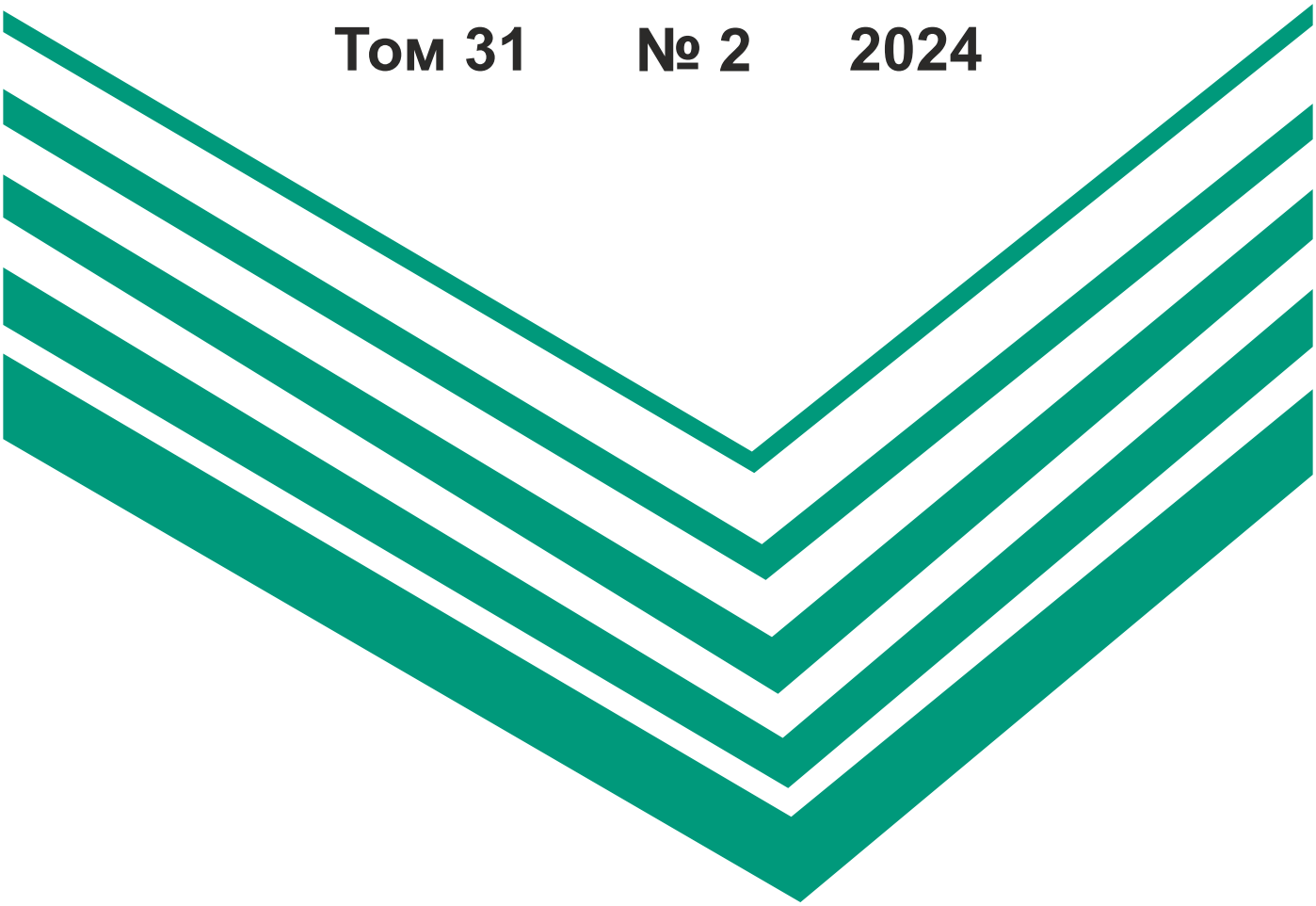
ISSN 2949-5598

# ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 2 2024



Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель–июнь 2024. Т. 31, № 2. С. 144–154

УДК 519.17 DOI: 10.33048/daio.2024.31.766

# О СЛОЖНОСТИ МЕТОДА ПОСЛЕДОВАТЕЛЬНОГО ОПРОБОВАНИЯ

*В. М. Фомичёв*[1,2]

[1] ООО «Код Безопасности»,
1-й Нагатинский пр-д, 10, стр. 1, 115230 Москва, Россия
[2] Институт проблем информатики ФИЦ «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, 119333 Москва, Россия
E-mail: fomichev.2016@yandex.ru

**Аннотация.** Система $m$ булевых уравнений может быть решена методом последовательного опробования с помощью $m$-шагового алгоритма, где на $i$-м шаге опробуются значения всех переменных, существенных для первых $i$ уравнений, и ложные решения отбраковываются по правым частям уравнений, $i = 1, \ldots, m$. Оценка сложности метода, зависящая от структуры множеств существенных переменных уравнений, достигает минимума при некоторых перестановках уравнений системы. Предложен алгоритм оптимальной перестановки уравнений, минимизирующей среднюю вычислительную сложность алгоритма в естественных вероятностных предположениях. В ряде случаев оптимальные перестановки определены неоднозначно, и их нахождение является вычислительно сложным. Метод последовательного опробования вырождается в полный перебор, если каждое уравнение системы зависит существенно от всех переменных. Приведён пример построения оптимальной перестановки. Табл. 2, ил. 1, билиогр. 11.

**Ключевые слова:** булева функция, существенная переменная, решётка подмножеств множества, цепь в решётке.

## Введение

Решение системы булевых уравнений в общем случае относится к задачам высокой сложности [1]. Для решения системы с $n$ неизвестными требуется до $2^n$ операций опробования значений неизвестных.

Сложность решения некоторых частных классов систем булевых уравнений оценивается как полиномиальная или субэкспоненциальная. Большое число работ посвящено решению линейных систем булевых уравнений, где мотивацией было обобщение и улучшение характеристик метода

Гаусса и других методов [2, 3]. Активно исследовались методы линеаризации, направленные на сведение решения нелинейной системы к некоторому числу линейных систем [4, 5]. Средняя сложность решения треугольных систем $n$ уравнений от $n$ переменных в естественной вероятностной модели близка к $2n$ [5]. Со сложностью порядка $\sqrt{2^n}$ методом согласования(англ. meet in the middle of attack) решается широкий класс систем, например системы уравнений, в которых АНФ каждой функции системы разлагается в сумму двух многочленов от непересекающихся подмножеств переменных; варианты этого метода описаны в [5–7].

Имеется также ряд исследований, претендующих на достаточно высокую степень общности в связи с классом решаемых систем уравнений. Их задача — выявить параметры систем уравнений, определяющие сложность решения, что позволяет конструктивно описать некоторые классы систем уравнений с оценкой сложности решения ниже тривиальной оценки $2^n$ [8–11].

Метод последовательного опробования применим к любой системе булевых уравнений, однако не для всех систем он эффективен, т. е. не для всех систем его сложность ниже сложности полного опробования вариантов решения системы. Для систем уравнений, в которых некоторые функции зависят не от всех переменных, показано, что с помощью перестановки уравнений системы можно достичь определённого приближения к треугольной системе уравнений и минимизации сложности метода последовательного опробования. Предложен алгоритм построения оптимальной перестановки уравнений на основе анализа множеств существенных переменных всех функций системы и приведён пример.

## 1. Постановка задачи

Требуется решить систему $m$ булевых уравнений

$$f_j(x_1, \ldots, x_n) = a_j, \quad j = 1, \ldots, m, \tag{1}$$

где $a_j \in \{0,1\}$, $f_j\colon \{0,1\}^n \to \{0,1\}$ — булевы функции, возможно существенно зависящие не от всех переменных, при этом каждая переменная существенна хотя бы для одной из функций в левой части системы. *Решением системы* (1) называется любой набор значений переменных $(x_1, \ldots, x_n) \in \{0,1\}^n$, при котором выполняется каждое уравнение системы. Остальные наборы называются *ложными решениями.* Отнесение набора к множеству ложных решений называют *отбраковкой.*

Пусть $Q_r = (q_1, \ldots, q_r)$ — бесповторная упорядоченная выборка $r \in \{1, \ldots, m\}$ чисел из множества $\{1, \ldots, m\}$, а $\{Q_r\} = \{q_1, \ldots, q_r\}$ — множество элементов выборки $Q_r$. Выборки $Q_r$ и $Q'_r$ назовём *односоставными,* если $\{Q_r\} = \{Q'_r\}$.

Перестановку $Q = Q_m = (q_1, \ldots, q_m)$ чисел $1, \ldots, m$ назовём *маркером* алгоритма решения системы (1). Маркер $Q$ однозначно определяет перестановку уравнений системы (1).

Для решения системы (1) применим $m$-шаговый алгоритм последовательного опробования(а. п. о.) с маркером $Q = (q_1, \ldots, q_m)$, который последовательно бракует ложные решения по уравнениям: сначала с номером $q_1$, затем с номером $q_2$ и т. д., наконец с номером $q_m$.

Задача состоит в том, чтобы найти маркер для а. п. о. с наименьшей вычислительной сложностью; назовём его *оптимальным маркером* (о. м.) для системы (1).

## 2. Алгоритм последовательного опробования

Пусть $S(j)$ — множество номеров всех существенных переменных булевой функции $f_j(x_1, \ldots, x_n)$ в левой части системы (1), $j = 1, \ldots, m$. Для маркера $Q = (q_1, \ldots, q_m)$ обозначим

$$\Delta_1(Q) = S(q_1),$$
$$\Delta_r(Q) = S(q_r) \setminus (S(q_1) \cup \cdots \cup S(q_{r-1})), \quad 2 \leqslant r \leqslant m,$$
$$n_r(Q) = |\Delta_r(Q)|, \quad r = 1, \ldots, m.$$

Для краткости не указываем зависимость множеств и величин от выборки $Q$ (т. е. $\Delta_r(Q) = \Delta_r$ и $n_r(Q) = n_r$), если корректность рассуждений не нарушается.

Опишем а. п. о. $A(Q)$ с маркером $Q$ и оценим его сложность, измеряемую числом операций отбраковки наборов значений некоторых переменных из $\{x_1, \ldots, x_n\}$ по одному из уравнений системы (1). Например, если $S(j) = \{i_1, \ldots, i_k\}$, $j \in \{1, \ldots, m\}$, то игнорируя несущественные переменные, имеем $f_j(x_1, \ldots, x_n) = f_j(x_{i_1}, \ldots, x_{i_k})$. Тогда одна операция состоит в проверке для произвольного набора двоичных констант $(\beta_{i_1}, \ldots, \beta_{i_k})$ выполнения равенства

$$f_j(\beta_{i_1}, \ldots, \beta_{i_k}) = a_j. \tag{2}$$

Если (2) не верно, то набор $(\beta_{i_1}, \ldots, \beta_{i_k})$ «забракован по $j$-му уравнению»; в противном случае набор «не забракован по $j$-му уравнению», и далее для этого набора или его пополнения некоторым числом булевых констант проверяется выполнимость другого уравнения.

**Алгоритм** $A(Q)$ (с маркером $Q = (q_1, \ldots, q_m)$)

Шаг 1. Опробуются все наборы значений $n_1$ переменных с номерами из $S(q_1)$, и ложные наборы бракуются по уравнению с номером $q_1$.

Шаг $r \geqslant 2$. Каждый не отбракованный на $(r-1)$-м шаге набор

1) бракуется по уравнению с номером $q_r$, если $\Delta_r = \varnothing$;

2) пополняется $2^{n_r}$ наборами значений переменных с номерами из $\Delta_r$, если $\Delta_r \neq \varnothing$, и пополненные наборы значений переменных бракуются по уравнению с номером $q_r$.

При $r < m$ для каждого неотбракованного набора значений переменных выполняется шаг $r+1$. При $r = m$ каждый неотбракованный набор значений переменных $(x_1, \ldots, x_n) \in \{0,1\}^n$ является решением системы уравнений (1).

Конец.

Оценим среднюю сложность $T(Q)$ алгоритма $A(Q)$ решения случайной системы (1) при следующих условиях:

1) правая часть $(a_1, \ldots, a_m) \in \{0,1\}^m$ системы (1) выбрана случайно и равновероятно;

2) при любом $j \in \{1, \ldots, m\}$ равенство (2) выполняется с вероятностью $\frac{1}{2}$ для любого двоичного набора $(\beta_{i_1}, \ldots, \beta_{i_k})$;

3) уравнения системы (1) независимы: при случайном наборе значений переменных вероятность выполнения любого уравнения не зависит от выполнимости других уравнений при этом наборе значений;

4) наборы значений переменных независимы: вероятность выполнения любого уравнения при случайном наборе значений переменных не зависит от выполнимости этого уравнения при любом другом наборе.

В этих условиях среднее число решений системы (1) равно $2^{n-m}$.

Пусть $T(Q)$ обозначает среднюю вычислительную сложность а. п. о. $A(Q)$, $T_r(Q)$ — среднее число операций при выполнении $r$-го шага а. п. о., а $M_r(Q)$ — среднее число неотбракованных наборов по завершении шага $r$ алгоритма. Из описания алгоритма $A(Q)$ следует, что

$$\sum_{1 \leqslant r \leqslant m} n_r(Q) = n, \tag{3}$$

$$T_r(Q) = M_{r-1}(Q) \cdot 2^{n_r},$$

$$M_r(Q) = M_{r-1}(Q) \cdot 2^{n_r - 1}, \quad 1 \leqslant r \leqslant m,$$

где $M_0(Q) = 1$. Так как $T(Q) = \sum\limits_{1 \leqslant r \leqslant m} T_r(Q)$, получаем

$$T(Q) = \sum_{1 \leqslant r \leqslant m} M_{r-1}(Q) \cdot 2^{n_r}. \tag{4}$$

Отсюда средняя сложность а. п. о. $A(Q)$ зависит от разбиения (3) числа $n$ на $m$ неотрицательных целых слагаемых $n_1(Q), \ldots, n_m(Q)$.

## 3. Оптимальный маркер

Пусть $R_n^m$ — множество разбиений натурального числа $n$ на $m$ неотрицательных целых слагаемых. Определим расстояние $\rho(\overline{n}, \overline{n}')$ между

разбиениями $\overline{n} = (n_1, \ldots, n_m)$, $\overline{n}' = (n'_1, \ldots, n'_m) \in R_n^m$ равенством

$$\rho(\overline{n}, \overline{n}') = \sum_{1 \leqslant i \leqslant m} |n_i - n'_i|.$$

Разбиения $\overline{n}$ и $\overline{n}'$ назовём *соседними,* если $\rho(\overline{n}, \overline{n}') = 2$. Для соседних разбиений множество разностей $\{n_1 - n'_1, \ldots, n_m - n'_m\}$ состоит из одной единицы, одной «минус единицы» и $m - 2$ нулей. Заметим, что множество $R_n^m$ линейно упорядочено лексикографически.

Определим бинарное отношение $\leqslant$ на множестве $R_n^m$. Для $\overline{n}, \overline{n}' \in R_n^m$ положим $\overline{n} \leqslant \overline{n}'$ тогда и только тогда, когда имеется цепь разбиений $(\overline{n}^{(1)}, \ldots, \overline{n}^{(t)})$, $t > 1$, такая, что $\overline{n}^{(1)} = \overline{n}$, $\overline{n}^{(t)} = \overline{n}'$, а $\overline{n}^{(j)}$ и $\overline{n}^{(j+1)}$ соседние, $j = 1, \ldots, t-1$, причём разбиение $\overline{n}^{(j)}$ лексикографически меньше разбиения $\overline{n}^{(j+1)}$.

В силу (3) маркер $Q$ однозначно определяет разбиение $\overline{n}(Q) = (n_1(Q), \ldots, n_m(Q)) \in R_n^m$. Для краткости пишем $\overline{n}(Q) = \overline{n}$, $\overline{n}(Q') = \overline{n}'$.

**Теорема 1.** *Если $\overline{n} \leqslant \overline{n}'$ для маркеров $Q$ и $Q'$, то $T(Q) < T(Q')$.*

Доказательство. Если разбиения $\overline{n}, \overline{n}'$ соседние, то $\rho(\overline{n}, \overline{n}') = 2$, и для некоторых $1 \leqslant k < l \leqslant m$, $n_k \geqslant 1$ разбиения имеют вид

$$\overline{n} = (n_1, \ldots n_{k-1}, n_k, n_{k+1}, \ldots, n_{l-1}, n_l, n_{l+1}, \ldots, n_m),$$
$$\overline{n}' = (n_1, \ldots, n_{k-1}, n_k + 1, n_{k+1}, \ldots, n_{l-1}, n_l - 1, n_{l+1}, \ldots, n_m).$$

Тогда для среднего числа неотбракованных наборов $M_r$ после шага $r$ а. п. о. верно равенство

$$M_r(Q) = \begin{cases} M_r(Q') & \text{при } r = 1, \ldots, k-1, l, \ldots, m, \\ \frac{1}{2} M_r(Q') & \text{при } r = k, \ldots, l-1, \end{cases} \tag{5}$$

при этом в силу (4) и (5)

$$T(Q') - T(Q) = \sum_{k \leqslant r \leqslant l-1} \frac{M_r(Q')}{2} > 0,$$

т. е. для соседних наборов теорема верна.

Если $\overline{n}$, $\overline{n}'$ не соседние, то по определению отношения $\leqslant$ в $R_n^m$ имеется цепь разбиений $(\overline{n}^{(1)}, \ldots, \overline{n}^{(t)})$, $t > 1$, такая, что $\overline{n}^{(1)} = \overline{n}$, $\overline{n}^{(t)} = \overline{n}'$, причём разбиения $\overline{n}^{(j)}$, $\overline{n}^{(j+1)}$ соседние и $\overline{n}^{(j)}$ лексикографически меньше $\overline{n}^{(j+1)}$, $j = 1, \ldots, t-1$. Тогда в соответствии с доказанным получаем

$$TQ) = T(\overline{n}^{(1)}) < T(\overline{n}^{(2)}) < \cdots < T(\overline{n}^{(t)}) = T(Q').$$

Теорема 1 доказана.

Заметим, что множество $S^{\langle m \rangle} = \{S(1), \ldots, S(m)\}$, порождаемое системой уравнений (1), частично упорядочено (образует ч. у. м.) относительно теоретико-множественного включения.

**Теорема 2.** *Если* $Q = (q_1, \ldots, q_m)$ *— о. м., то* $S(q_1)$ *— минимальный элемент ч. у. м.* $S^{\langle m \rangle}$.

Доказательство. Если множество $S^{\langle m \rangle}$ — антицепь в решётке (булеане) $2^{\{1,\ldots,m\}}$, то все элементы $S^{\langle m \rangle}$ минимальные, и утверждение теоремы тривиально. Если $S^{\langle m \rangle}$ не антицепь, то покажем, что $S(q_1)$ минимальный элемент в этом множестве.

Предположим, напротив, что в $S^{\langle m \rangle}$ имеется цепь с минимальным элементом $S(q_h) \subset S(q_1)$ при некотором $h \geqslant 2$. Без ограничения общности будем считать, что $h = 2$, и пусть $u = |S(q_2)|$, $v = |S(q_1)|$. Тогда $u < v$ и можно построить цепь разбиений из $R_n^m$

$$\overline{n}^{(0)} \leqslant \overline{n}^{(1)} \leqslant \ldots \leqslant \overline{n}^{(v-u)}$$

такую, что $\overline{n}^{(t)} = (u + t, v - u - t, n_3, \ldots, n_m)$, $t = 0, 1, \ldots, v - u$. В этой цепи $\overline{n}^{(v-u)} = \overline{n}(Q)$, а разбиение $\overline{n}^{(0)} = \overline{n}(Q')$ соответствует маркеру $Q' = (q_2, q_1, q_3, \ldots, q_m)$. В соответствии с теоремой 1 получаем $T(Q') < T(Q)$, что противоречит оптимальности маркера $Q$. Следовательно, $S(q_1)$ — минимальный элемент в $S^{\langle m \rangle}$. Теорема 2 доказана.

Теорема 2 определяет $m$-шаговый алгоритм $A(S^{\langle m \rangle})$ нахождения о. м. Обозначим через $M(X)$ множество минимальных элементов ч. у. м. $X$, а для маркера $Q_r$ положим $S^{\langle m \rangle \setminus Q_r} = S^{\langle m \rangle} \setminus \{S(q_j)\}_{j=1}^{r}$, $1 \leqslant r < m$.

**Алгоритм** $A(S^{\langle m \rangle})$

Шаг 1. Вычислить $M(S^{\langle m \rangle})$ и сформировать варианты для выборки $Q_1 = (q_1)$, где $S(q_1) \in M(S^{\langle m \rangle})$.

Шаг $r$ ($2 \leqslant r \leqslant m - 1$). Для каждой выборки $Q_{r-1} = (q_1, \ldots, q_{r-1})$, сформированной на шаге $r - 1$, сформировать варианты выборки $Q_r = (q_1, \ldots, q_{r-1}, q_r)$, где $S(q_r) \in M(S^{\langle m \rangle \setminus Q_{r-1}})$.

Шаг $m$. Для каждой выборки $Q_{m-1} = (q_1, \ldots, q_{m-1})$, сформированной на шаге $m - 1$, сформировать маркер $Q = (q_1, \ldots, q_{m-1}, q_m)$, где $q_m \notin \{Q_{m-1}\}$.

**Замечание 1.** О. м. $Q = (q_1, \ldots, q_m)$ является элементом декартова произведения $M(S^{\langle m \rangle}) \times M(S^{\langle m \rangle \setminus Q_1}) \times \cdots \times M(S^{\langle m \rangle \setminus Q_{m-1}})$ и в общем случае определён неоднозначно. Многозначность о. м. в худшем случае, когда $S(1) = \cdots = S(m) = \{1, \ldots, n\}$, оценивается величиной $m!$.

Многозначность и сложность поиска о. м. для систем уравнений (1) снижается, в частности, при следующих условиях:

1) если на шаге $r \geqslant 2$ сформированы односоставные выборки $Q_r$ и $Q'_r$, то $M(S^{\langle m \rangle \setminus Q_r}) = M(S^{\langle m \rangle \setminus Q'_r})$, следовательно, на шаге $r + 1$ достаточно найти минимальный элемент лишь для одной из этих выборок;

2) если в $S^{\langle m \rangle}$ имеются одинаковые множества.

Оценим возможное снижение трудоёмкости в связи со вторым условием. Для системы уравнений (1) числа $i$ и $j$, $1 \leqslant i, j \leqslant m$, назовём *эквивалентными,* если $S(i) = S(j)$; в этом случае пишем $i \sim j$.

Пусть $u$ — число классов эквивалентности в $\{1, \ldots, m\}$ отношения $\sim$, $1 \leqslant u \leqslant m$, которые обозначим через $H_s$, $h_s = |H_s|$, $s = 1, \ldots, u$.

Маркеры $Q$ и $Q'$ назовём *эквивалентными,* если $\overline{n} = \overline{n}'$, т. е. одинаковы соответствующие им разбиения $\overline{n}, \overline{n}' \in R_n^m$; при этом пишем $Q \sim Q'$.

**Теорема 3.** *При разбиении на классы эквивалентности*

$$\{1, \ldots, m\} = H_1 \cup \cdots \cup H_u$$

*число попарно неэквивалентных о. м. не превышает* $\frac{m!}{h_1! \ldots h_u!}$.

Доказательство. Пусть на $r$-м шаге алгоритма $A(S^{\langle m \rangle})$ сформирована выборка $Q_r = (q_1, \ldots, q_{r-1}, q_r)$, где $q_r \in H_s$ и $q_1, \ldots, q_{r-1} \notin H_s$. Тогда на шагах $r+1, \ldots, r+h_s-1$ дополним $Q_r$ остальными элементами класса $H_s$. Это соответствует алгоритму $A(S^{\langle m \rangle})$, так как из того, что $S(q_r) \in M(S^{\langle m \rangle \setminus Q_{r-1}})$, следует $S(q) \in M(S^{\langle m \rangle \setminus Q_{r-1}})$ для любого $q \in H_s \setminus \{q_r\}$. Тем самым при любом порядке выбора элементов из $H_s$ на шагах $r, \ldots, r+h_s-1$ алгоритма $A(S^{\langle m \rangle})$ получаем эквивалентные маркеры. Отсюда вытекает справедливость оценки из условия теоремы. Теорема 3 доказана.

**Следствие 1.** *Если отношение эквивалентности на* $\{1, \ldots, m\}$ *нетривиально* (*не вырождается в равенство*), *то алгоритм* $A(S^{\langle m \rangle})$ *сводится к поиску о. м. для подсистемы, в которой номера уравнений образуют трансверсал этого отношения* (*т. е. систему представителей классов эквивалентности*).

**Замечание 2.** Если на шагах $r \geqslant 1, r+1, \ldots, r+h_s-1$ алгоритма $A(S^{\langle m \rangle})$ элементы о. м. $Q$ равны элементам множества $H_s$, $s \in \{1, \ldots, u\}$, то $n_{r+1}(Q) = \cdots = n_{r+h_s-1}(Q) = 0$.

**Пример 1.** Для класса систем пяти уравнений $f_j(x_1, \ldots, x_6) = a_j$, $j = 1, \ldots, 5$, определим о. м. и среднюю сложность решения при известном о. м. Множества $S(1), \ldots, S(5)$ даны в табл. 1. Найдём о. м. $Q = (q_1, \ldots, q_5)$ с учётом того, что $4 \sim 5$.

*Таблица 1*

**Множества $S(j)$ системы функций**

| $j$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $S(j)$ | $\{1,2\}$ | $\{1,2,4\}$ | $\{3,5\}$ | $\{3,4,5\}$ | $\{3,4,5\}$ |

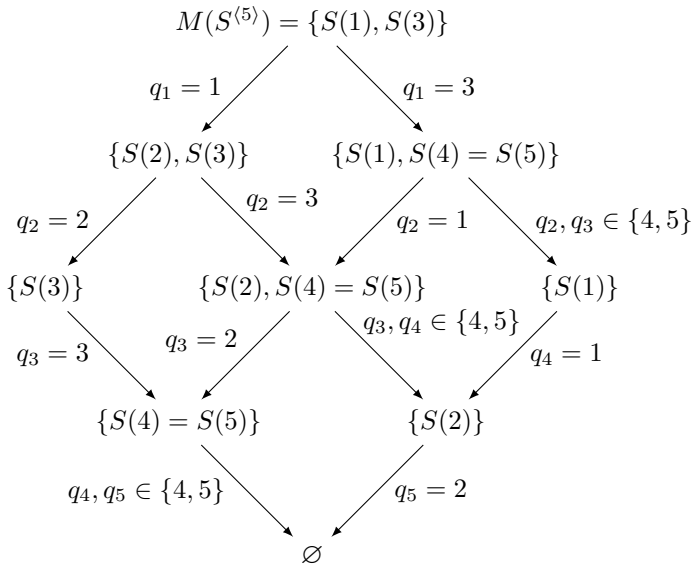



*Рис. 1.* Схема алгоритма $A(S^{\langle m\rangle})$ для системы из примера 1

Работа алгоритма $A(S^{\langle m\rangle})$ представлена в виде схемы на рис. 1. В каждой вершине указано множество минимальных элементов $M(S^{\langle m\rangle \setminus Q_{r-1}})$, рассматриваемое на текущем шаге $r$. На дугах отмечены элементы формируемых маркеров.

*Таблица 2*

**Характеристики маркеров системы**

| № | Маркер $Q$ | Разбиение числа 5 | $T(Q)$ |
|---|---|---|---|
| 1 | $(12345) \sim (12354)$ | $2+1+2+0+0$ | 22 |
| 2 | $(13452) \sim (13542)$ | $2+2+1+0+0$ | 26 |
| 3 | $(31245) \sim (31254)$ | $2+2+1+0+0$ | 26 |
| 4 | $(31452) \sim (31542)$ | $2+2+1+0+0$ | 26 |
| 5 | $(34512) \sim (35412)$ | $2+1+0+2+0$ | 16 |

В табл. 2 приведены «кандидаты» в о. м., соответствующие им разбиения числа 5 и средняя вычислительная сложность а. п. о. для каждого маркера. В 5-й строке можно видеть два эквивалентных о. м. со сложностью $T(Q) = 16$. Отметим, что средняя сложность решения системы уравнений методом полного перебора равна 62.

**Финансирование работы**

Исследование выполнено за счёт бюджетов организаций, обозначенных автором на первой странице статьи. Дополнительных грантов на проведение или руководство этим исследованием получено не было.

**Конфликт интересов**

Автор заявляет, что у него нет конфликта интересов.

**Литература**

1. **Гэри М., Джонсон Д.** Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 416 с.
2. **Коновальцев И. В.** Об одном алгоритме решения систем линейных уравнений в конечных полях // Проблемы кибернетики. Т. 19. М.: Физматгиз, 1967. С. 269–274.
3. **Strassen V.** Gaussian elimination is not optimal // Numer. Math. 1969. V. 13. P. 354–356.
4. **Courtois N. T.** Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt // Information security and cryptology — ICISC 2002. Rev. Pap. 5th Int. Conf. (Seoul, Korea, Nov. 28–29, 2002). Heidelberg: Springer, 2003. P. 182–199. (Lect. Notes Comput. Sci.; V. 2587).
5. **Фомичёв В. М.** Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.
6. **Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2002. 1040 с.
7. **Mercle R. C., Hellman M.** On the security of multiple encryption // Commun. ACM. 1981. V. 24, No. 7. P. 465–467.
8. **Мелузов А. С.** Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных // Дискрет. математика. 2011. Т. 23, № 4. С. 66–79.
9. **Фомичёв В. М.** Оценка характеристик нелинейности итеративных преобразований векторного пространства // Дискрет. анализ и исслед. операций. 2020. Т. 27, № 4. С. 131–151.
10. **Rivest R. L.** Cryptography // Handbook of theoretical computer science. V. A: Algorithms and complexity. Cambridge, MA: MIT Press, 1990. P. 617–755.
11. **Stinson D. R.** Cryptography: Theory and practice. Boca Raton: CRC Press, 1995. 434 p.

*Фомичёв Владимир Михайлович*

Статья поступила
30 марта 2023 г.
После доработки —
17 октября 2023 г.
Принята к публикации
22 декабря 2023 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
April–June 2024. Vol. 31, No. 2. P. 144–154

UDC 519.17 DOI: 10.33048/daio.2024.31.766

# ON THE COMPLEXITY OF THE SEQUENTIAL SAMPLING METHOD

*V. M. Fomichev*[1,2]

[1] Security Code LLC,
10 Bld. 1 Pervyi Nagatinskii Driveway, 115230 Moscow, Russia
[2] Institute of Informatics Problems of FRC CSC RAS,
44 Bld. 2 Vavilov Street, 119333 Moscow, Russia
E-mail: fomichev.2016@yandex.ru

**Abstract.** A system of $m$ Boolean equations can be solved by a sequential sampling method using an $m$-step algorithm, where at the $i$-th step the values of all variables essential for the first $i$ equations are sampled and false solutions are rejected based on the right-hand sides parts of the equations, $i = 1, \ldots, m$. The estimate of the complexity of the method depends on the structure of the sets of essential variables of the equations and attains its minimum after some permutation of the system equations. For the optimal permutation of equations we propose an algorithm that minimizes the average computational complexity of the algorithm under natural probabilistic assumptions. In a number of cases, the construction of such a permutation is computationally difficult; in this connection, other permutations are proposed which are computed in a simpler way but may lead to nonoptimal estimates of the complexity of the method. The results imply conditions under which the sequential sampling method degenerates into the exhaustive search method. An example of constructing an optimal permutation is given. Tab. 2, illustr. 1, biliogr. 11.

**Keywords:** Boolean function, essential variable, subset lattice of a set, chain in a lattice.

## References

1. **M. R. Garey** and **D. S. Johnson,** *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979; Mir, Moscow, 1982 [Russian]).

English transl.: *Journal of Applied and Industrial Mathematics* **18** (2), 227–233 (2024), DOI: 10.1134/S1990478924020054.

2. **I. V. Konovaltsev,** An algorithm for solving systems of linear equations in finite fields, in *Problems of Cybernetics,* Vol. 19 (Fizmatgiz, Moscow, 1967), pp. 269–274 [Russian].
3. **V. Strassen,** Gaussian elimination is not optimal, *Numer. Math.* **13**, 354–356 (1969).
4. **N. T. Courtois,** Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, in *Information Security and Cryptology — ICISC 2002* (Rev. Pap. 5th Int. Conf., Seoul, Korea, Nov. 28–29, 2002) (Springer, Heidelberg, 2003), pp. 182–199 (Lect. Notes Comput. Sci., Vol. 2587).
5. **V. M. Fomichev,** *Methods of Discrete Mathematics in Cryptology* (DIALOG-MIFI, Moscow, 2010) [Russian].
6. **B. Schneier,** *Applied Cryptography. Protocols, Algorithms, and Source Code in C* (Wiley, Hoboken, NJ, 1993; TRIUMF, Moscow, 2002 [Russian]).
7. **R. C. Mercle** and **M. Hellman,** On the security of multiple encryption, *Commun. ACM* **24** (7), 465–467 (1981).
8. **A. S. Meluzov,** On construction of efficient algorithms for solving systems of polynomial Boolean equations by testing a part of variables, *Diskretn. Mat.* **23** (4), 66–79 (2011) [Russian] [*Discrete Math. Appl.* **21** (3), 381–395 (2011)].
9. **V. M. Fomichev,** Estimating nonlinearity characteristics for iterative transformations of a vector space, *Diskretn. Anal. Issled. Oper.* **27** (4), 131–151 (2020) [Russian] [*J. Appl. Ind. Math.* **14** (4), 610–622 (2020)].
10. **R. L. Rivest,** Cryptography, in *Handbook of Theoretical Computer Science,* Vol. A: Algorithms and Complexity (MIT Press, Cambridge, MA, 1990), pp. 617–755.
11. **D. R. Stinson,** *Cryptography: Theory and Practice* (CRC Press, Boca Raton, 1995).

*Vladimir M. Fomichev*

Received March 30, 2023
Revised October 17, 2023
Accepted December 22, 2023