Math-Net.Ru

Общероссийский математический портал

А. В. Тарасов, Параметры метода максимального правдоподобия при его использовании для решения систем дважды биконкативных уравнений с искаженными правыми частями, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 3, 79–100

DOI: <https://doi.org/10.4213/mvk333>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 15:58:55

**Параметры метода максимального правдоподобия
при его использовании для решения систем
дважды биюнктивных уравнений
с искаженными правыми частями**

А. В. Тарасов

ООО «Центр сертификационных исследований», Москва

Получено 29.IV.2019

Аннотация. Рассматривается задача решения заведомо совместных систем булевых уравнений с дважды биюнктивными функциями, со случайным выбором неизвестных в каждом уравнении и с искаженными правыми частями. Оцениваются основные параметры процедуры решения таких систем методом максимального правдоподобия.

Ключевые слова: булева функция, биюнктивная функция, система булевых уравнений

Parameters of the maximum likelihood method applied to the solution of systems of twice bijunctive equations with corrupted right-hand sides

A. V. Tarasov

LLC «Sertification Research Center», Moscow

Abstract. We consider the problem of solution of surely solvable systems of Boolean equations with twice bijunctive functions, random independent sets of unknowns in all equations and corrupted right-hand sides. Estimates of the main parameters of the procedure of solution searching for such systems by means of maximum likelihood method are obtained.

Keywords: Boolean function, bijunctive function, system of Boolean equations

Введение

Одним из наиболее известных классов быстро решаемых систем булевых уравнений является класс систем линейных уравнений. Алгоритмам их решения посвящено большое количество работ. Однако существуют и другие классы систем, для которых полиномиальна как минимум задача распознавания совместности. Например, такими являются классы систем булевых уравнений без ограничений на выбор неизвестных над так называемыми классами Шефера (см. [1–3]). Введем необходимые определения.

Пусть $F = \{f_j(x_1, \dots, x_{k_j}), j \in J\}$ – набор булевых функций, $X = \{x_i, i = 1, 2, 3, \dots\}$. Символом $[F]_{NC}$ обозначим класс систем уравнений следующего вида:

$$\left\{ f_{s_i}(x_{s_{i,1}}, \dots, x_{s_{i,k_{s_i}}}) = 1, i = 1, \dots, t, \right. \quad (1)$$

где $t \in N$, $s_i \in J$, $f_{s_i} \in F$, $x_{s_{i,m}} \in X$, $m = \overline{1, k_{s_i}}$.

Класс булевых функций F называется *полиномиально решаемым*, если выполнены два условия.

1. Существует полиномиальный алгоритм распознавания совместности систем вида (1) из $[F]_{NC}$. При этом под полиномиальным алгоритмом понимается алгоритм решения задачи, временная сложность которого полиномиально зависит от длины записи задачи (см., например, [2, 3]).

2. Существует алгоритм, который в случае совместности системы вида (1) последовательно без повторений находит все решения системы, причем сложность построения первого и каждого последующего решений ограничена одним и тем же полиномом от длины записи системы.

В работах [1, 2] описаны все классы булевых функций, порождающие полиномиально решаемые системы булевых уравнений вида $[F]_{NC}$. Эти классы называются *классами Шефера*. Одним из таких классов функций является класс *Ві* булевых бионктивных функций. Он включает в себя функции, представимые в виде 2-КНФ:

$$f(x_1, \dots, x_n) = \bigwedge_{j=1}^p x_{r_j}^{b_j} \bigwedge_{i=1}^t (x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}}). \quad (2)$$

Ряд аналитических свойств функций из этого класса изучен в [2, 4, 5].

При анализе систем булевых уравнений иногда возникает необходимость составления и решения систем уравнений с искаженными правыми частями. Данной проблематике посвящен ряд работ (см., например,

[7,8]), и задача анализа таких систем представляется существенно более сложной, поскольку понятие *решения* системы выходит за рамки определения вектора, удовлетворяющего всем уравнениям. Как правило, такая система является несовместной, и в качестве решения выбирается вектор, дающий наименьшее значение статистики «невязки» (числа невыполненных равенств). Такой вектор может не совпадать с вектором, на котором была получена правая часть системы до ее искажения.

Если в системе уравнений с искаженными правыми частями в левых частях стоят функции из классов Шефера, то возникают следующие вопросы:

1. Применимы ли известные методы решения систем из полиномиально решаемых классов к поиску решений систем с искаженными правыми частями?
2. С какой вероятностью будет найдено правильное решение системы, т. е. набор значений неизвестных, по которому была получена правая часть до ее искажения, если в левых частях уравнений стоят функции из классов Шефера?

Для того чтобы можно было применять известные методы решения неискаженных систем, необходимо рассматривать подклассы классов Шефера, замкнутые относительно операции инверсии функций. К таким классам относится класс дважды бионктивных функций. Булева функция $f(x_1, \dots, x_n)$ называется *дважды бионктивной*, если $f \in Bi$ и $f \oplus 1 \in Bi$.

Для произвольной функции $f(x_1, \dots, x_n)$ обозначим через $[f]$ класс функций от n переменных, получаемых из функции f с помощью перестановки переменных, навешивания на них отрицаний и инверсии всей функции (легко видеть, что $[f] = [f]_{Q_n} \cup [f \oplus 1]_{Q_n}$, где $[f]_{Q_n}$ – класс функций, эквивалентных f относительно группы Джевонса). Такой класс функций назовем *классом геометрической эквивалентности* функции f . В [2] показано, что дважды бионктивными являются все функции от одной и двух переменных, а среди функций от большего числа переменных такими являются только функции от трех или четырех переменных, причем (с точностью до класса геометрической эквивалентности) их всего пять. Перечислим их:

$$\begin{aligned}
f_1 &= x_1(x_2 \vee x_3), \\
f_2 &= (x_1 \vee x_2)(x_1 \vee x_3)(x_2 \vee x_3), \\
f_3 &= (x_1 \vee x_2)(\bar{x}_1 \vee x_3), \\
f_4 &= (x_1 \vee x_2)(x_3 \vee x_4), \\
f_5 &= (x_1 \vee x_2)(x_2 \vee x_3)(x_3 \vee x_4).
\end{aligned} \tag{3}$$

Целью настоящей работы является изучение некоторых свойств систем уравнений с искажениями, порождаемых этими функциями.

1. Системы уравнений с искаженными правыми частями со случайным выбором неизвестных и метод максимального правдоподобия

Понятие системы булевых уравнений с искаженными правыми частями введем в соответствии с [8]. В дальнейшем будем пользоваться терминологией этой работы. *Системой булевых уравнений с искаженными правыми частями* называется система уравнений следующего вида:

$$\{h_i(x_1, \dots, x_n) = a_i, \quad i = \overline{1, t}, \tag{4}$$

где $h_i, i = \overline{1, t}$, – булевы функции от n переменных, $a_i = h_i(x^{(0)}) \oplus \gamma_i$, $i = \overline{1, t}$, причем $x^{(0)} = (x_1^0, \dots, x_n^0)$ – неизвестный вектор, который, следуя терминологии [8], будем называть *истинным решением* системы (4), а $\bar{\gamma} = (\gamma_1, \dots, \gamma_t)$ – двоичный вектор ошибок, компоненты которого являются реализациями независимых одинаково распределенных случайных величин:

$$\gamma_i \sim \begin{pmatrix} 0 & 1 \\ 1-p & p \end{pmatrix}, \quad p < 0.5, \quad i = 1, 2, \dots, t.$$

В рамках рассматриваемой задачи будем считать, что

$$h_i = g(x_{s_{i,1}}, \dots, x_{s_{i,r}}), \tag{5}$$

где g – фиксированная булева функция от r переменных, а $\bar{s}_i = (s_{i,1}, \dots, s_{i,r})$, $i \in \overline{1, t}$, – выборки без возвращения по r элементов из множества $\{1, 2, \dots, n\}$, независимые в совокупности и имеющие равномерное распределение на множестве $N(n, r)$ из всех $(n)_r = n(n-1) \dots (n-r+1)$ таких выборок.

Обозначив при заданных функции $g(x_1, \dots, x_r)$ и числе неизвестных n

$$\Sigma = N(n, r)^t, \quad \Gamma = V_t,$$

получаем, что система (4) представляет собой реализацию случайной величины, определенной на множестве $\Omega = \Sigma \times \Gamma$.

Основной метод решения систем вида (4) (см. [7, 8]), называемый *методом максимального правдоподобия*, состоит в переборе векторов $z = (z_1, \dots, z_n) \in V_n$, подсчете для каждого вектора статистики «невязки» вида

$$S(z) = \sum_{i=1}^t (h_i(z) \oplus a_i) \quad (6)$$

и выборе того значения z , для которого данная статистика имеет наименьшее значение. Естественно, что при этом надежность метода, т. е. вероятность того, что истинное решение имеет наименьшее значение статистики (6), зависит от числа уравнений, свойств собственно функции g , вероятности p и свойств истинного решения системы. В частности, при достаточно большом размере системы (4) с большой вероятностью в качестве оптимального будет выбрано истинное решение $x^{(0)}$. В данном разделе нас интересуют именно эти параметры в случае, когда исходная функция g выбирается из множества дважды бионктивных функций.

Для простоты рассуждений всюду далее будем предполагать, что истинное решение $x^{(0)} = (x_1^0, \dots, x_n^0)$ системы (4) имеет следующую структуру:

$$x_1^0 = \dots = x_{n_1}^0 = 1, \quad x_{n_1+1}^0 = \dots = x_n^0 = 0, \quad n_1 = [\theta \cdot n], \quad (7)$$

где $\theta \in (0, 1)$ — константа, а $[\cdot]$ обозначает целую часть числа.

Обозначим через $\mathcal{P}$ вероятность правильного решения системы (4) методом максимального правдоподобия, т. е. вероятность того, что минимальное значение статистики (6) достигается на векторе $x^{(0)}$. Тогда

$$\mathcal{P} = \mathbf{P} \left(S(x^{(0)}) < \min_{z \neq x^{(0)}} S(z) \right) = 1 - \mathbf{P} \left(\max_{z \neq x^{(0)}} (S(x^{(0)}) - S(z)) \geq 0 \right). \quad (8)$$

Оценив вероятность $\mathbf{P} \left(\max_{z \neq x^{(0)}} (S(x^{(0)}) - S(z)) \geq 0 \right)$ сверху, получим нижнюю оценку для $\mathcal{P}$. Рассуждения, приводящие к выводу неравенства (14) (см. ниже), принадлежат Г.В. Балакину и приводятся для полноты изложения.

При фиксированном наборе выборок $\sigma = (\bar{s}_1, \dots, \bar{s}_t) \in \Sigma$, определяющем выбор неизвестных в уравнениях системы (4) (т. е. при фиксированной левой части системы (4)), рассмотрим произвольный фиксиро-

ванный вектор $z = (z_1, \dots, z_n)$, для которого $\|x^{(0)} \oplus z\| = k, 1 \leq k \leq n$. Положим $T_\sigma(z) = \{i : h_i(x^{(0)}) \neq h_i(z)\}$ и $\tau_\sigma(z) = |T_\sigma(z)|$.

Тогда

$$\begin{aligned} S(x^{(0)}) - S(z) &= \sum_{i=1}^t \gamma_i - \left(\sum_{i \notin T_\sigma(z)} \gamma_i + \sum_{i \in T_\sigma(z)} (1 - \gamma_i) \right) \\ &= \sum_{i \in T_\sigma(z)} (2 \cdot \gamma_i - 1) = 2 \cdot \sum_{i \in T_\sigma(z)} \gamma_i - \tau_\sigma(z). \end{aligned}$$

В этом случае условная вероятность события $\{S(x^{(0)}) - S(z) \geq 0\}$ при фиксированном σ имеет вид

$$\mathbf{P}(S(x^{(0)}) - S(z) \geq 0 | \sigma) = \mathbf{P}\left(\sum_{i \in T_\sigma(z)} \gamma_i \geq \frac{\tau_\sigma(z)}{2}\right) = \tilde{p}(\tau_\sigma(z)),$$

где функция $\tilde{p}(\tau) = \mathbf{P}\left(\sum_{i=1}^t \gamma_i \geq \frac{\tau}{2}\right)$, $\tau \in \overline{1, t}$, зависит только от распределения случайных величин $\gamma_1, \dots, \gamma_t$ и не зависит от σ . Тогда

$$\begin{aligned} \mathbf{P}\left(\max_{z \neq x^{(0)}} (S(x^{(0)}) - S(z)) \geq 0 | \sigma\right) &= \mathbf{P}\left(\bigcup_{z \neq x^{(0)}} (S(x^{(0)}) - S(z) \geq 0) | \sigma\right) \\ &\leq \sum_{z \neq x^{(0)}} \mathbf{P}(S(x^{(0)}) - S(z) \geq 0 | \sigma) = \sum_{z \neq x^{(0)}} \mathbf{P}\left(\sum_{i \in T_\sigma(z)} \gamma_i \geq \frac{\tau_\sigma(z)}{2}\right) \\ &= \sum_{z \neq x^{(0)}} \sum_{j=0}^t I(\tau_\sigma(z) = j) \tilde{p}(j) = \sum_{z \neq x^{(0)}} \tilde{p}(\tau_\sigma(z)), \end{aligned}$$

где $I(\tau_\sigma(z) = j)$ — индикатор того, что $\tau_\sigma(z) = j$ при заданном фиксированном z и наборе выборов $\sigma = (\bar{s}_1, \dots, \bar{s}_t)$.

Пусть $P(\sigma)$ — вероятность появления набора выборов σ , равная $((n)_r)^{-t}$. Осредняя по всем вариантам наборов выборов $\sigma \in \Sigma$,

получаем:

$$\begin{aligned}
 \mathbf{P} \left(\max_{z \neq x^{(0)}} (S(x^{(0)}) - S(z)) \geq 0 \right) &= \sum_{\sigma \in \Sigma} P(\sigma) \mathbf{P} \left(\max_{z \neq x^{(0)}} (S(x^{(0)}) - S(z)) \geq 0 \middle| \sigma \right) \\
 &\leq \sum_{\sigma \in \Sigma} \mathbf{P}(\sigma) \sum_{z \neq x^{(0)}} \sum_{j=0}^t I(\tau_{\sigma}(z) = j) \tilde{p}(j) = \sum_{j=0}^t \tilde{p}(j) \sum_{z \neq x^{(0)}} \sum_{\sigma \in \Sigma} P(\sigma) I(\tau_{\sigma}(z) = j) \\
 &= \sum_{k=1}^n \sum_{z: \|z \oplus x^{(0)}\| = k} \sum_{j=0}^t \tilde{p}(j) \sum_{\sigma \in \Sigma} P(\sigma) I(\tau_{\sigma}(z) = j).
 \end{aligned} \tag{9}$$

Оценим сверху вероятности $\tilde{p}(j)$. Очевидно, что

$$\tilde{p}(j) = \sum_{i=\lfloor \frac{j+1}{2} \rfloor}^n \binom{j}{i} p^i \cdot (1-p)^{j-i}, \tag{10}$$

где $\lfloor x \rfloor$ обозначает целую часть x .

Поскольку $0 \leq p < \frac{1}{2} < 1-p \leq 1$, максимальным членом вида $p^i \cdot (1-p)^{j-i}$ в каждой сумме является первый.

Пусть j нечетно. Тогда, поскольку $\sum_{i=\lfloor \frac{j+1}{2} \rfloor}^j \binom{j}{i} = 2^{j-1}$, то

$$\tilde{p}(j) \leq 2^{j-1} \cdot p^{\frac{j+1}{2}} \cdot (1-p)^{\frac{j-1}{2}} = \frac{1}{2} \sqrt{\frac{4^j \cdot p^j \cdot (1-p)^j \cdot p}{1-p}} \leq \left(\sqrt{4p(1-p)} \right)^j.$$

Пусть j четно. Тогда из (10)

$$\begin{aligned}
 \tilde{p}(j) &= \binom{j}{\frac{j}{2}} p^{\frac{j}{2}} (1-p)^{\frac{j}{2}} + \sum_{i=\frac{j}{2}+1}^n \binom{j}{i} p^i \cdot (1-p)^{j-i} \\
 &\leq \binom{j}{\frac{j}{2}} p^{\frac{j}{2}} (1-p)^{\frac{j}{2}} + 2^{j-1} p^{\frac{j}{2}} (1-p)^{\frac{j}{2}} \sqrt{\frac{p}{1-p}}.
 \end{aligned}$$

Поскольку $\frac{p}{1-p} < 1$ и при четном j верно неравенство $\binom{j}{\frac{j}{2}} \leq 2^{j-1}$, получаем:

$$\tilde{p}(j) \leq 2^{j-1} p^{\frac{j}{2}} (1-p)^{\frac{j}{2}} + 2^{j-1} p^{\frac{j}{2}} (1-p)^{\frac{j}{2}} = \left(\sqrt{4p(1-p)} \right)^j.$$

Обозначим $\delta = 1 - \sqrt{4p(1-p)}$. Тогда $0 < \delta < 1$ и в обоих случаях

получаем неравенство $\tilde{p}(j) \leq (1 - \delta)^j$. Тогда из (9):

$$\begin{aligned} & \mathbf{P} \left(\max_{x \neq x^{(0)}} (S(x^{(0)}) - S(x)) \geq 0 \right) \\ & \leq \sum_{k=1}^n \sum_{z: \|z \oplus x^{(0)}\| = k} \sum_{j=0}^t (1 - \delta)^j \sum_{\sigma} P(\sigma) I(\tau_{\sigma}(z) = j). \end{aligned} \quad (11)$$

Рассмотрим такой вектор z , что $\|x^{(0)} \oplus z\| = k$ и $|\{l: x_l^0 = 1, z_l = 0\}| = k_0$, $0 \leq k_0 \leq k$. Обозначим через $p^{(i)}(z, k, k_0) = \mathbf{P}(h_i(x^{(0)}) \neq h_i(z))$, $1 \leq i \leq t$, вероятность того, что $h_i(x^{(0)}) \neq h_i(z)$ при случайной выборке $\bar{s}_i = (s_{i,1}, \dots, s_{i,r})$ и фиксированных $x^{(0)}$ и z . Тогда

$$\begin{aligned} p^{(i)}(z, k, k_0) &= \sum_{\bar{s}_i \in N(n,r): g(x_{s_{i,1}}^0, \dots, x_{s_{i,r}}^0) \neq g(z_{s_{i,1}}, \dots, z_{s_{i,r}})} P(\bar{s}_i) \\ &= \frac{1}{(n)_r} \sum_{\bar{s}_i \in N(n,r)} I\{g(x_{s_{i,1}}^0, \dots, x_{s_{i,r}}^0) \neq g(z_{s_{i,1}}, \dots, z_{s_{i,r}})\} \\ &= \frac{|\{\bar{s}_i \in N(n,r) : g(x_{s_{i,1}}^0, \dots, x_{s_{i,r}}^0) \neq g(z_{s_{i,1}}, \dots, z_{s_{i,r}})\}|}{(n)_r}. \end{aligned} \quad (12)$$

Легко видеть, что данная вероятность не зависит от $i \in \{1, 2, \dots, t\}$, а поскольку выборки $\bar{s}$ независимы и имеют равномерное распределение на множестве $N(n, r)$, то она зависит только от параметров k и k_0 . Поэтому в дальнейшем мы ее будем обозначать $p(k, k_0)$.

В этом случае

$$\begin{aligned} \sum_{\sigma} P(\sigma) I(\tau_{\sigma}(z) = j) &= \sum_{M \subset \bar{1}, t, |M|=j} \prod_{i \in M} p(k, k_0) \prod_{i \notin M} (1 - p(k, k_0)) \\ &= \binom{t}{j} p^j(k, k_0) (1 - p(k, k_0))^{t-j}. \end{aligned}$$

Значит,

$$\begin{aligned} \sum_{j=0}^t \tilde{p}(j) \sum_{\sigma} P(\sigma) I(\tau_{\sigma}(z) = j) &\leq \sum_{j=0}^t \binom{t}{j} p^j(k, k_0) (1 - p(k, k_0))^{t-j} (1 - \delta)^j \\ &= (p(k, k_0)(1 - \delta) + (1 - p(k, k_0)))^t = (1 - p(k, k_0)\delta)^t. \end{aligned} \quad (13)$$

Тогда, с учетом (11),

$$\begin{aligned} \mathcal{P} &\geq 1 - \sum_{z \neq x^{(0)}} \sum_{j=0}^t \tilde{p}(j) \sum_{\sigma} P(\sigma) I(\tau_{\sigma}(z) = j) \\ &\geq 1 - \sum_{k=1}^n \sum_{z: \|z \oplus x^{(0)}\| = k} (1 - p(k, k_0) \delta)^t \\ &= 1 - \sum_{k=1}^n \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} (1 - p(k, k_0) \cdot \delta)^t. \end{aligned}$$

Таким образом, верно неравенство

$$\mathcal{P} \geq 1 - \sum_{k=1}^n \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} (1 - p(k, k_0) \delta)^t. \quad (14)$$

Для получения дальнейших результатов будем оценивать вероятности $p(k, k_0)$ снизу при заданной функции g . Это позволит применить неравенство (14) и получить содержательную оценку для $\mathcal{P}$.

При фиксированных векторах $x^{(0)}, z$ будем считать, что выполнены соотношения

$$\begin{aligned} z_1 &= \dots = z_{n_1 - k_0} = z_{n_1 + 1} = \dots = z_{n_1 + k - k_0} = 1, \\ z_{n_1 - k_0 + 1} &= \dots = z_{n_1} = z_{n_1 + k - k_0 + 1} = \dots = z_n = 0. \end{aligned}$$

Определим множество

$$S = \{ (i_1, \dots, i_r) \in N(n, r) : g(x_{i_1}^0, \dots, x_{i_r}^0) \neq g(z_{i_1}, \dots, z_{i_r}) \}.$$

Тогда из (12) получаем

$$p(k, k_0) = \frac{|S|}{(n)_r}. \quad (15)$$

Для удобства дальнейших рассуждений определим множества

$$\begin{aligned} M_0 &= \{i \in \overline{1, n} : x_i^0 = z_i = 1\}, \quad M_1 = \{i \in \overline{1, n} : x_i^0 = 1, z_i = 0\}, \\ M_2 &= \{i \in \overline{1, n} : x_i^0 = 0, z_i = 1\}, \quad M_3 = \{i \in \overline{1, n} : x_i^0 = z_i = 0\}. \end{aligned}$$

Через m_0, m_1, m_2, m_3 обозначим мощности этих множеств. Очевидно, что

$$m_0 = n_1 - k_0, m_1 = k_0, m_2 = k - k_0, m_3 = n - n_1 + k_0 - k. \quad (16)$$

На основе равенства (15) доказывается следующий простой факт.

Утверждение 1. Для всех $k, k_0 : 1 \leq k \leq n, 0 \leq k_0 \leq k$ верно неравенство

$$p(k, k_0) \leq 1 - \frac{(n - k)_r}{(n)_r}. \quad (17)$$

Доказательство. Из равенства (15) и определения множества S следует, что

$$\begin{aligned} p(k, k_0) &= \frac{|S|}{(n)_r} \\ &= 1 - \frac{|\{(i_1, \dots, i_r) \in N(n, r) : g(x_{i_1}^0, \dots, x_{i_r}^0) = g(z_{i_1}, \dots, z_{i_r})\}|}{(n)_r}. \end{aligned} \quad (18)$$

Положим $S' = N(n, r) \setminus S$ и $S'' = \{(i_1, \dots, i_r) \in N(n, r) : z_{i_1} = x_{i_1}^0, \dots, z_{i_r} = x_{i_r}^0\}$. Если $(i_1, \dots, i_r) \in S''$, то очевидно, что $g(x_{i_1}^0, \dots, x_{i_r}^0) = g(z_{i_1}, \dots, z_{i_r})$. Тогда $S'' \subset S'$ и верны соотношения

$$p(k, k_0) = 1 - \frac{|S'|}{(n)_r} \leq 1 - \frac{|S''|}{(n)_r}. \quad (19)$$

Осталось заметить, что набор $(i_1, \dots, i_r) \in S''$ тогда и только тогда, когда индексы $i_1, \dots, i_r$ выбираются из множества $M_0 \cup M_3$. Поэтому $|S''| = (|M_0 \cup M_3|)_r = (m_0 + m_3)_r = A_{n-k}^r$. Отсюда

$$p(k, k_0) \leq 1 - \frac{(n - k)_r}{(n)_r}. \quad (20)$$

Утверждение доказано. $\square$

Утверждение 1 позволяет получить оценку величины $p(k, k_0)$ сверху. Однако для получения оценки вероятности $\mathcal{P}$ по формуле (14) необходимо получить нижнюю оценку для этой вероятности. Для этого сначала докажем следующее утверждение.

Утверждение 2. Пусть множество S не пусто и содержит набор $(i_1, \dots, i_r)$. Определим числа $q_1, \dots, q_r \in \{0, 1, 2, 3\}$ по принципу: $i_1 \in M_{q_1}, \dots, i_r \in M_{q_r}$. Тогда для всякого такого вектора $(j_1, \dots, j_r) \in N(n, r)$, что $j_1 \in M_{q_1}, \dots, j_r \in M_{q_r}$, выполнено условие $(j_1, \dots, j_r) \in S$.

Доказательство. Пусть $(i_1, \dots, i_r) \in S$. Тогда

$$x_{i_1}^0 = x_{j_1}^0, \dots, x_{i_r}^0 = x_{j_r}^0, \quad z_{i_1} = z_{j_1}, \dots, z_{i_r} = z_{j_r}.$$

Поэтому $g(x_{j_1}^0, \dots, x_{j_r}^0) = g(x_{i_1}^0, \dots, x_{i_r}^0)$ и $g(z_{j_1}, \dots, z_{j_r}) = g(z_{i_1}, \dots, z_{i_r})$, откуда и следует наше утверждение. $\square$

Смысл утверждения 2 состоит в том, что для получения оценок вероятностей $p(k, k_0)$ достаточно задавать не само множество S , а множество вида

$$\tilde{S} = \{(q_1, \dots, q_r) \in \{0, \dots, 3\}^r : S \cap (M_{q_1} \times \dots \times M_{q_r}) \neq \emptyset\}.$$

При этом

$$|S| = \sum_{(q_1, \dots, q_r) \in \tilde{S}} |\{(M_{q_1} \times \dots \times M_{q_r}) \cap N(n, r)\}|. \quad (21)$$

Смысл введенных множеств $M_{q_1}, \dots, M_{q_r}$ состоит в том, что они показывают соотношения между компонентами векторов $x^{(0)}$ и z при выполнении равенства

$$g(x_{i_1}^0, \dots, x_{i_r}^0) \oplus g(z_{i_1}, \dots, z_{i_r}) = 1. \quad (22)$$

Иначе говоря, если выполнено равенство (22), то для значений $i_1, \dots, i_r$ будут выполняться равенства $q_l = 3 - (2 \cdot x_{i_l}^0 + z_{i_l})$, $l = 1, 2, \dots, r$. Соответственно, множество $\tilde{S}$ содержит в себе все возможные варианты соотношений между элементами векторов $x^{(0)}$ и z , при которых выполнено (22).

Множество $\tilde{S}$ можно определить следующим образом. Рассмотрим вектор $\tilde{q} = (q_1, \dots, q_r) \in (\mathbb{Z}_4)^r$, принадлежащий r -й декартовой степени множества $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Для булевой функции $g(x_1, \dots, x_r)$ определим функцию $\varphi_g : (\mathbb{Z}_4)^r \rightarrow \{0, 1\}$ следующим образом. Пусть векторы $y = (y_1, \dots, y_r)$ и $z = (z_1, \dots, z_r)$ составлены соответственно из старших и младших битов компонент вектора $\tilde{q}$. Значение функции φ_g вычисляется по формуле

$$\varphi_g(q_1, \dots, q_r) = g(y_1, \dots, y_r) \oplus g(z_1, \dots, z_r).$$

Таким образом, множество $\tilde{S}$ является множеством истинности функции φ_g . Определенное таким образом для функции g множество $\tilde{S}$ по сути представляет собой объединение декартовых произведений:

$$\tilde{S} = (E_g \times \bar{E}_g) \cup (\bar{E}_g \times E_g),$$

где E_g – множество истинности функции g , а $\bar{E}_g = V_r \setminus E_g$. Значения векторов $\tilde{q} \in \tilde{S}$ для дважды биюнктивных функций с учетом их кратности приведены в приложении.

Слагаемые из суммы в правой части равенства (21), соответствующие векторам $\tilde{q} = (q_1, \dots, q_r) \in \tilde{S}$, обозначим через $a(\tilde{q})$. Очевидно, что каждое слагаемое в (21) зависит не от порядка элементов $q_1, \dots, q_r$, а от того, сколько раз среди них встречается каждое из чисел $0, 1, 2, 3$. Например, если $r = 3$, $\tilde{q} = (q_1, q_2, q_3) \in \tilde{S}$, $\tilde{s} = (1, 1, 2)$, то выполнено равенство

$$a(\tilde{q}) = |M_1| \cdot (|M_1| - 1) \cdot |M_2|.$$

В этом случае очевидно следующее утверждение.

Утверждение 3. *Во введенных обозначениях верно равенство*

$$|S| = \sum_{\tilde{q} \in \tilde{S}} a(\tilde{q}). \quad (23)$$

Прежде чем перейти к изложению основных теорем, сделаем очевидное замечание. Рассуждения относительно статистики (6), проведенные при выводе формул (7)–(15), верны не только для систем (4) с условием (5), но и для более широкого класса систем вида (4), удовлетворяющих условиям

$$h_i \in [g], \quad i = \overline{1, t}, \quad (24)$$

где $[g]$ — класс геометрической эквивалентности функции g , рассматриваемой как функция от n переменных.

2. Параметры метода максимального правдоподобия при его применении к заведомо совместным системам уравнений с искаженными правыми частями, порождаемым дважды биюнктивными функциями

Теорема 1. *Пусть для заведомо совместной системы уравнений с искаженными правыми частями вида (4) выполняются условия: функции $h^{(i)}$, $i = \overline{1, t}$, принадлежат $[f_1]$, $0 < \theta < 1$, $0 \leq p < 0.5$, $\delta = 1 - \sqrt{4p(1-p)}$ и*

$$t = 3n(\ln n + w_n)/(\delta\theta),$$

где $w_n = o(\ln n)$, $w_n > 2$, $n \rightarrow \infty$. Тогда при $n \rightarrow \infty$ вероятность правильного решения системы (4) методом максимального правдоподобия удовлетворяет неравенству

$$\mathcal{P} \geq 2 - e^{-w_n}.$$

Доказательство. Получим нижнюю оценку вероятности $p(k, k_0)$. В самом деле,

$$\begin{aligned} p(k, k_0) &= \mathbf{P} \left(h_i(x^{(0)}) \neq h_i(z) \right) \\ &= \mathbf{P} \left(h_i(x^{(0)}) = 0, h_i(z) = 1 \right) + \mathbf{P} \left(h_i(x^{(0)}) = 1, h_i(z) = 0 \right). \end{aligned}$$

Пусть $k_0 \leq \frac{k}{2}$. Тогда, поскольку $h(x_1, x_2, x_3) = x_1(x_2 \vee x_3)$, то

$$\begin{aligned} p(k, k_0) &\geq \mathbf{P} \left(x_{j_1}^{(0)} = 1, x_{j_2}^{(0)} \vee x_{j_3}^{(0)} = 1, z_{j_1} = 0 \right) \\ &\quad + \mathbf{P} \left(z_{j_1} = 1, z_{j_2} \vee z_{j_3} = 1, x_{j_1}^{(0)} = 0 \right) \\ &\geq \mathbf{P} \left(x_{j_1}^{(0)} = 1, x_{j_2}^{(0)} = 1, z_{j_1} = 0 \right) + \mathbf{P} \left(z_{j_1} = 1, z_{j_2} = 1, x_{j_1}^{(0)} = 0 \right) \\ &= (m_1(m_0 + m_1 - 1)(n - 2) + m_2(m_0 + m_2 - 1)(n - 2)) \cdot (n)_3^{-1} \\ &= (k_0(n\theta - 1)(n - 2) + (k - k_0)(n\theta + k - 2k_0 - 1)(n - 2)) \cdot (n)_3^{-1} \\ &= (k(n\theta - 1)(n - 2) + (k - k_0)(k - 2k_0)(n - 2)) \cdot (n)_3^{-1} \\ &\geq k(n\theta - 1)(n - 2) \cdot (n)_3^{-1} = \frac{k(n\theta - 1)}{n(n - 1)} \geq \frac{k\theta}{3n} \end{aligned}$$

при достаточно больших n .

Если же $k_0 > \frac{k}{2}$, то

$$\begin{aligned} p(k, k_0) &\geq \mathbf{P} \left(x_{j_1}^{(0)} = 1, x_{j_2}^{(0)} = 1, z_{j_1} = 0 \right) \\ &= (m_1(m_0 + m_1 - 1)(n - 2)) \cdot (n)_3^{-1} \\ &= \frac{k_0(n\theta - 1)(n - 2)}{(n)_3} \geq \frac{k(n\theta - 1)(n - 2)}{2n(n - 1)(n - 2)} \geq \frac{k(n\theta - 1)(n - 2)}{2n(n - 1)(n - 2)} \geq \frac{k\theta}{3n} \end{aligned}$$

при достаточно больших n .

Тогда

$$\begin{aligned} \mathcal{P} &\geq 1 - \sum_{k=1}^n \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} (1 - p(k, k_0)\delta)^t \\ &\geq 1 - \sum_{k=1}^n \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} \left(1 - \frac{k\theta\delta}{3n} \right)^t \\ &= 1 - \sum_{k=1}^n \left(1 - \frac{k\theta\delta}{3n} \right)^t \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} = 1 - \sum_{k=1}^n \binom{n}{k} \left(1 - \frac{k\theta\delta}{3n} \right)^t. \end{aligned}$$

Воспользовавшись известными неравенствами $1 - x < e^{-x}$ при $0 < x < 1$ и $\binom{n}{k} \leq \frac{n^k}{k!}$, а также выражением для t , получаем:

$$\begin{aligned} \mathcal{P} &> 1 - \sum_{k=1}^n \frac{n^k}{k!} \exp\left(-\frac{3n(\ln n + w_n)}{\theta\delta} \frac{k\theta\delta}{3n}\right) = 1 - \sum_{k=1}^n \frac{n^k}{k!} \exp(-k \ln n - kw_n) \\ &= 1 - \sum_{k=1}^n \frac{\exp(-kw_n)}{k!} \geq 2 - \sum_{k=0}^{\infty} \frac{\exp(-w_n)^k}{k!} = 2 - e^{-w_n}. \end{aligned}$$

Полученная нижняя оценка является содержательной, поскольку по условию теоремы $w_n > 2 > \ln \ln 2$, откуда $0 < 2 - e^{-w_n} < 1$. $\square$

Теорема 2. Пусть для заведомо совместной системы уравнений с искоженными правыми частями вида (4) выполняются следующие условия: функции $h^{(i)}$, $i = \overline{1, t}$, принадлежат $[f_2]$, $0 < \theta < 1$, $0 \leq p < 0.5$, $\delta = 1 - \sqrt{4p(1-p)}$ и

$$t = n(\ln n + w_n)/[3\theta(1-\theta)\delta],$$

где $w_n = o(\ln n)$, $w_n > 2$, $n \rightarrow \infty$. Тогда при $n \rightarrow \infty$ вероятность правильного решения системы (4) методом максимального правдоподобия удовлетворяет неравенству

$$\mathcal{P} \geq 2 - e^{-w_n}.$$

Доказательство. Рассмотрим неравенство (14):

$$\mathcal{P} \geq 1 - \sum_{k=1}^n \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1-p(k, k_0)\delta)^t.$$

Сумму в правой части этого неравенства обозначим через I . Тогда

$$\begin{aligned} I &= \sum_{1 \leq k < \ln n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1-p(k, k_0)\delta)^t \\ &\quad + \sum_{\ln n \leq k < \varepsilon \cdot n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1-p(k, k_0)\delta)^t \\ &\quad + \sum_{\varepsilon \cdot n \leq k \leq n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1-p(k, k_0)\delta)^t = I_1 + I_2 + I_3, \end{aligned} \tag{25}$$

где $0 < \varepsilon < 1$ — произвольное. Покажем, что при достаточно больших n основной вклад в эту сумму вносят слагаемые с малыми значениями k .

Для этого получим нижние оценки вероятностей $p(k, k_0)$. Сначала рассмотрим сумму I_2 . С учетом того, что функция f_2 – симметрическая, получаем, что

$$\begin{aligned} p(k, k_0) &\geq 6 \cdot \mathbf{P}(j_1 \in M_0, j_2 \in M_3, j_3 \in M_1 \cup M_2) \\ &= 6 \cdot \frac{1}{(n)_3} ((n_1 - k_0)(n - n_1 - (k - k_0))k) \\ &\geq 6 \cdot \frac{1}{(n)_3} kn^2(\theta - \varepsilon)(1 - \theta - \varepsilon) = 6k \frac{\theta(1 - \theta) - \varepsilon + \varepsilon^2}{n} + o\left(\frac{1}{n}\right). \end{aligned} \quad (26)$$

Выберем ε , удовлетворяющее неравенству $\varepsilon < 0.5 \cdot \theta(1 - \theta)$. Тогда

$$p(k, k_0) > 3 \cdot k \cdot \frac{\theta(1 - \theta)}{n} + o\left(\frac{1}{n}\right).$$

В таком случае

$$\begin{aligned} I_2 &= \sum_{\ln n \leq k < \varepsilon \cdot n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n - n_1}{k - k_0} (1 - p(k, k_0)\delta)^t \\ &\leq \sum_{\ln n \leq k < \varepsilon \cdot n} \binom{n}{k} \left(1 - \frac{kc}{n}\right)^t, \end{aligned}$$

где $c = 3\theta(1 - \theta)\delta > 0$. Воспользуемся асимптотикой для $\binom{n}{k}$, вытекающей из формулы Стирлинга (см., например, [9]):

$$\binom{n}{k} = \frac{1 + o(1)}{\sqrt{2\pi n \beta_k (1 - \beta_k)}} \cdot \exp\{-n[\beta_k \ln \beta_k + (1 - \beta_k) \ln(1 - \beta_k)]\}, \beta_k = \frac{k}{n},$$

и неравенством $1 - x < e^{-x}$. Тогда

$$\begin{aligned} I_2 &< \sum_{\ln n \leq k < \varepsilon \cdot n} \frac{\exp\{-n[\beta_k \ln \beta_k + (1 - \beta_k) \ln(1 - \beta_k)] - t\beta_k c\}}{\sqrt{2\pi n \beta_k (1 - \beta_k)}} \\ &= \sum_{\ln n \leq k < \varepsilon \cdot n} \frac{\exp\{-n[\beta_k \ln \beta_k + (1 - \beta_k) \ln(1 - \beta_k)] - n(\ln n + \omega_n)\beta_k\}}{\sqrt{2\pi n \beta_k (1 - \beta_k)}} \\ &\leq \sum_{\ln n \leq k < \varepsilon \cdot n} \frac{\exp\{-n[\beta_k \ln \beta_k + (1 - \beta_k) \ln(1 - \beta_k) + \beta_k \ln n]\}}{\sqrt{2\pi n \beta_k (1 - \beta_k)}}. \end{aligned}$$

Далее, заметим, что функция $\beta(1 - \beta)$ возрастает при $0 < \beta < 0.5$. Поэтому функция $\frac{1}{\sqrt{2\pi n\beta_k(1-\beta_k)}}$ убывает при $\frac{\ln n}{n} \leq \beta_k < \varepsilon$ и верны неравенства

$$\frac{1}{\sqrt{2\pi n\beta_k(1-\beta_k)}} \leq \frac{1}{\sqrt{2\pi n\frac{\ln n}{n}(1-\frac{\ln n}{n})}} < \frac{1}{\sqrt{\pi \ln n}}.$$

Кроме того, легко видеть, что $\beta \ln \beta + (1 - \beta) \ln(1 - \beta) < 0$ при $0 < \beta < 1$. Более того, эта функция убывает при $0 < \beta < 0.5$ и возрастает при $0.5 < \beta < 1$. Поэтому при $\frac{\ln n}{n} \leq \beta_k < \varepsilon$

$$\begin{aligned} & \exp\{-n[\beta_k \ln \beta_k + (1 - \beta_k) \ln(1 - \beta_k) + \beta_k \ln n]\} \\ & < \exp\{-n[\varepsilon \ln \varepsilon + (1 - \varepsilon) \ln(1 - \varepsilon) + \beta_k \ln n]\} = \exp\{\lambda n\}, \end{aligned}$$

где $0 < \lambda < 1$. Но тогда

$$I_2 < \frac{1}{\sqrt{\pi \ln n}} \cdot n\varepsilon \cdot \exp\{n[\lambda - \ln^2 n]\} = \frac{\varepsilon}{\sqrt{\pi \ln n}} \cdot \exp\{\ln n + n\lambda - n \ln^2 n\} \rightarrow 0$$

при $n \rightarrow \infty$.

Рассмотрим сумму

$$I_3 = \sum_{\varepsilon \cdot n \leq k \leq n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1 - p(k, k_0)\delta)^t.$$

Так же, как в неравенстве (26), получаем:

$$\begin{aligned} p(k, k_0) & \geq 6 \cdot \mathbf{P}(j_1 \in M_0, j_2 \in M_3, j_3 \in M_1 \cup M_2) \\ & = 6 \cdot \frac{1}{(n)_3} ((n_1 - k_0)(n - n_1 - (k - k_0))k), \end{aligned} \quad (27)$$

и при этом $k \geq n\varepsilon$.

Пусть $k_0 \leq \frac{k}{2}$. Тогда $k - k_0 > \frac{k}{2} \geq \frac{n\varepsilon}{2}$. В этом случае

$$p(k, k_0) \geq \frac{6 \cdot \varepsilon \cdot n\theta \cdot [n(1 - \theta) - \frac{n\varepsilon}{2}]}{(n)_3}.$$

Поскольку $\varepsilon < 0.5 \cdot \theta(1 - \theta)$ и $0 < \theta < 1$, то $\frac{\varepsilon}{2} < \frac{1 - \theta}{4}$ и $n(1 - \theta) - \frac{n\varepsilon}{2} > \frac{n(1 - \theta)}{2}$.

Поэтому

$$p(k, k_0) \geq \frac{3n^3 \cdot \varepsilon \cdot \theta \cdot (1 - \theta)}{(n)_3} > 3\theta(1 - \theta)\varepsilon.$$

Аналогичное неравенство легко доказывается и для случая $k_0 > \frac{k}{2}$. Поэтому верны неравенства

$$\begin{aligned}
 I_3 &\leq \sum_{\varepsilon \cdot n \leq k \leq n} \binom{n}{k} (1 - 3\theta(1 - \theta)\varepsilon\delta)^t \\
 &< \sum_{0 \leq k \leq n} \binom{n}{k} (1 - 3\theta(1 - \theta)\varepsilon\delta)^t = 2^n \cdot (1 - 3\theta(1 - \theta)\varepsilon\delta)^t \\
 &< 2^n \cdot \exp\{-3t\theta(1 - \theta)\varepsilon\delta\} = 2^n \cdot \exp\{-3t\theta(1 - \theta)\varepsilon\delta\} \\
 &< 2^n \cdot \exp\{-\varepsilon n \ln n\} = \exp\{n \ln 2 - \varepsilon n \ln n\} \rightarrow 0, \quad n \rightarrow \infty.
 \end{aligned} \tag{28}$$

Таким образом, основной вклад в сумму I вносят слагаемые с малыми k . Получим нижнюю оценку вероятности $p(k, k_0)$ при $k < \ln n$. Для этого воспользуемся равенством (15) и утверждением 2. Вычислим мощность множества $S = \{(i_1, \dots, i_r) : g(x_{i_1}^0, \dots, x_{i_r}^0) \neq g(z_{i_1}, \dots, z_{i_r})\}$ при $g = f_2$. Воспользуемся множеством $\tilde{S}$ и равенством (21). Множество $\tilde{S}$ приведено в приложении. В результате получаем:

$$\begin{aligned}
 |S| &= m_0(m_1)_2 + m_0m_1m_3 + m_0(m_2)_2 + m_0m_2m_3 + m_0m_3m_1 \\
 &+ m_0m_3m_2 + m_0(m_1)_2 + m_0m_1m_3 + m_0(m_1)_2 + (m_1)_3 + (m_1)_2m_2 \\
 &+ (m_1)_2m_3 + (m_1)_2m_2 + m_1(m_2)_2 + m_0m_1m_3 + (m_1)_2m_3 \\
 &+ m_0(m_2)_2 + m_0m_2m_3 + m_2(m_1)_2 + m_1(m_2)_2 + (m_2)_2m_0 \\
 &+ (m_2)_2m_1 + (m_2)_3 + (m_2)_2m_3 + m_2m_3m_0 + (m_2)_2m_3 + m_3m_0m_1 \\
 &+ m_3m_0m_2 + m_3m_1m_0 + m_3(m_1)_2 + m_3m_2m_0 + m_3(m_2)_2 \\
 &= 3m_0(m_1)_2 + 6m_0m_1m_3 + 6m_0m_2m_3 + 3m_0(m_2)_2 + 3(m_1)_2m_2 \\
 &+ 3(m_1)_2m_3 + 3m_1(m_2)_2 + 3(m_2)_2m_3 + (m_1)_3 + (m_2)_3.
 \end{aligned} \tag{29}$$

Проведя замену в соответствии с (16), получим:

$$\begin{aligned}
 |S| &= 3(n\theta - k_0)k_0(k_0 - 1) + 6(n\theta - k_0)k_0(n(1 - \theta) - k + k_0) \\
 &+ 6(n\theta - k_0)(k - k_0)(n(1 - \theta) - k + k_0) + 3(n\theta - k_0)(k - k_0)(k - k_0 - 1) \\
 &+ 3k_0(k_0 - 1)(k - k_0) + 3k_0(k_0 - 1)(n(1 - \theta) - k + k_0) \\
 &+ 3k_0(k - k_0)(k - k_0 - 1) + 3(k - k_0)(k - k_0 - 1)(n(1 - \theta) - k + k_0) \\
 &+ k_0(k_0 - 1)(k_0 - 2) + (k - k_0)(k - k_0 - 1)(k - k_0 - 2).
 \end{aligned}$$

Раскрывая скобки и воспользовавшись соотношениями

$$k < \ln n, k_0 < \ln n, k - k_0 < \ln n,$$

получаем:

$$p(k, k_0) = \frac{|S|}{(n)_3} = \frac{6k\theta(1-\theta)}{n} + o\left(\frac{\ln n}{n}\right) > \frac{3k\theta(1-\theta)}{n}.$$

Подставив полученное выражение в сумму I_1 , находим, что

$$I_1 < \sum_{1 \leq k < \ln n} \binom{n}{k} \left(1 - \frac{3k\theta(1-\theta)\delta}{n}\right)^t.$$

Теперь заметим, что

$$\left(1 - \frac{3k\theta(1-\theta)\delta}{n}\right)^t < \exp\left(-t \frac{3k\theta(1-\theta)\delta}{n}\right) = \exp(-k(\ln n + w_n)).$$

Значит,

$$I_1 < \sum_{1 \leq k < \ln n} \binom{n}{k} e^{-k(\ln n + w_n)}.$$

Но тогда, с учетом неравенства $\binom{n}{k} < \frac{n^k}{k!}$, получаем:

$$\begin{aligned} \mathcal{P} &\geq 1 - \sum_{1 \leq k < \ln n} \binom{n}{k} e^{-k(\ln n + w_n)} - I_2 - I_3 > 2 - \sum_{0 \leq k \leq n} \binom{n}{k} e^{-k(\ln n + w_n)} \\ &= 2 - \sum_{0 \leq k \leq n} \binom{n}{k} n^{-k} e^{-kw_n} > 2 - \sum_{k=0}^{\infty} \frac{n^k}{k!} n^{-k} e^{-kw_n} = 2 - e^{-w_n}. \end{aligned}$$

Содержательность полученной оценки доказывается аналогично теореме 1. $\square$

Теорема 3. Пусть для заведомо совместной системы уравнений с искаженными правыми частями вида (4) выполняются следующие условия: функции $h^{(i)}$, $i = \overline{1, t}$, принадлежат $[f_3]$, $0.3 < \theta < 0.7$, $0 \leq p < 0.5$, $\delta = 1 - \sqrt{4p(1-p)}$ и

$$t = n(\ln n + w_n)/[(1 + 2\theta - 2\theta^2)\delta],$$

где $w_n = o(\ln n)$, $w_n > 2$, $n \rightarrow \infty$. Тогда при $n \rightarrow \infty$ вероятность правильного решения системы (4) методом максимального правдоподобия удовлетворяет неравенству

$$\mathcal{P} \geq 2 - e^{-w_n}.$$

Доказательство. Найдем мощность множества S . В соответствии с приложением

$$\begin{aligned}
 |S| &= (m_0)_2 m_1 + (m_0)_2 m_2 + m_0 (m_1)_2 + m_0 m_1 m_2 + m_0 m_2 m_1 + m_0 (m_2)_2 \\
 &\quad + m_0 m_3 m_1 + m_0 m_3 m_2 + m_1 m_0 m_2 + m_1 m_0 m_3 + (m_1)_2 m_0 + (m_1)_3 \\
 &\quad + m_1 (m_2)_2 + m_1 m_2 m_3 + m_1 m_3 m_0 + (m_1)_2 m_3 + m_2 m_0 m_1 + m_2 m_0 m_3 \\
 &\quad + m_2 (m_1)_2 + m_2 m_1 m_3 + (m_2)_2 m_0 + (m_2)_3 + m_2 m_3 m_0 + (m_2)_2 m_3 \\
 &\quad + m_3 m_1 m_0 + m_3 (m_1)_2 + m_3 m_1 m_2 + (m_3)_2 m_1 \\
 &\quad + m_3 m_2 m_0 + m_3 m_2 m_1 + m_3 (m_2)_2 + (m_3)_2 m_2 \\
 &= 4m_0 m_1 m_2 + 4m_0 m_1 m_3 + 4m_0 m_2 m_3 + 4m_1 m_2 m_3 + 2(m_1)_2 m_3 \\
 &\quad + (m_0)_2 m_1 + (m_0)_2 m_2 + 2m_0 (m_1)_2 + 2m_0 (m_2)_2 + m_1 (m_3)_2 \\
 &\quad + (m_1)_3 + (m_2)_3 + m_1 (m_2)_2 + (m_1)_2 m_2 + 2(m_2)_2 m_3 + m_2 (m_3)_2 \\
 &= 4((m_0 + m_1)m_2 m_3 + m_0 m_1 (m_2 + m_3)) + 2(m_0 + m_3)((m_1)_2 + (m_2)_2) \\
 &\quad + ((m_0)_2 + (m_3)_2)(m_1 + m_2) + ((m_1)_2 + (m_2)_2)(m_1 + m_2 - 2) \\
 &\quad = 4((m_0 + m_1)m_2 m_3 + m_0 m_1 (m_2 + m_3)) \\
 &\quad + (2m_0 + m_1 + m_2 + 2m_3 - 2)((m_1)_2 + (m_2)_2) + ((m_0)_2 + (m_3)_2)(m_1 + m_2).
 \end{aligned}$$

В силу равенств (16) получаем:

$$\begin{aligned}
 |S| &= 4(n\theta(k - k_0)(n(1 - \theta) - k + k_0) + (n\theta - k_0)k_0 n(1 - \theta)) \\
 &\quad + (2n - k - 2)((k_0)_2 + (k - k_0)_2) + k((n\theta - k_0)_2 + (n(1 - \theta) - k + k_0)_2) \\
 &= n^2 k[1 + 2\theta - 2\theta^2] - 4n(\theta(k - k_0)^2 + k_0^2(1 - \theta)) \\
 &\quad + (2n - k - 2)(k_0(k_0 - 1) + (k - k_0)(k - k_0 - 1)) \\
 &\quad + k(k - n - 2n(k_0\theta + (k - k_0)(1 - \theta))) \\
 &= n^2 k[1 + 2\theta - 2\theta^2] + nk[4\theta k_0 - 2\theta k - 2k_0 - 3] + 4kk_0 - 4k_0^2 + 2k \\
 &\geq n^2 k[1 + 2\theta - 2\theta^2] + nk[4\theta k_0 - 2\theta k - 2k_0 - 3] + 2k.
 \end{aligned}$$

Отсюда

$$\begin{aligned}
 p(k, k_0) &= \frac{|S|}{(n)_3} \geq \frac{k[1 + 2\theta - 2\theta^2]}{n} + \frac{k[4\theta k_0 - 2\theta k - 2k_0 - 3]}{n^2} + \frac{2k}{n^3} \\
 &= \frac{k[1 + 2\theta - 2\theta^2]}{n} + \frac{k[(4\theta - 2)k_0 - 2\theta k]}{n^2} + O\left(\frac{1}{n}\right).
 \end{aligned}$$

Рассмотрим величину $p_1 = \frac{k[1+2\theta-2\theta^2]}{n} + \frac{k[(4\theta-2)k_0-2\theta k]}{n^2}$. При фиксированном k данная величина возрастает при $0 \leq k_0 \leq \min(k, n\theta)$ и, так как

$0.3 < \theta < 0.7$, то $1 - 2\theta^2 > 0$ и можно считать, что

$$p(k, k_0) \geq \frac{k}{n}(1 - 2\theta^2).$$

Если же $k < \ln n$, то

$$p(k, k_0) = \frac{k[1+2\theta-2\theta^2]}{n} + O\left(\frac{1}{n}\right).$$

Рассмотрим сумму I вида (25):

$$\begin{aligned} I &= \sum_{1 \leq k < \ln n} \sum_{k_0=0}^k \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1 - p(k, k_0)\delta)^t \\ &+ \sum_{\ln n \leq k < \varepsilon \cdot n} \sum_{k_0=0}^{\min(k, n\theta)} \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1 - p(k, k_0)\delta)^t \\ &+ \sum_{\varepsilon \cdot n \leq k \leq n} \sum_{k_0=0}^{\min(k, n\theta)} \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1 - p(k, k_0)\delta)^t = I_1 + I_2 + I_3. \end{aligned} \quad (30)$$

Аналогично доказательству теоремы 2 легко показать, что

$$I_1 < \sum_{1 \leq k < \ln n} \binom{n}{k} e^{-k(\ln n + w_n)}.$$

Далее, аналогично (27)

$$\begin{aligned} I_3 &= \sum_{\varepsilon \cdot n \leq k \leq n} \sum_{k_0=0}^{\min(k, n\theta)} \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} (1 - p(k, k_0)\delta)^t \\ &\leq \sum_{\varepsilon \cdot n \leq k \leq n} \sum_{k_0=0}^{\min(k, n\theta)} \binom{n_1}{k_0} \binom{n-n_1}{k-k_0} \left(1 - \frac{k}{n}(1 - 2\theta^2)\delta\right)^t \\ &\leq \sum_{\varepsilon \cdot n \leq k \leq n} \binom{n}{k} \left(1 - \frac{k}{n}(1 - 2\theta^2)\delta\right)^t \leq \sum_{1 \leq k \leq n} \binom{n}{k} (1 - \varepsilon(1 - 2\theta^2)\delta)^t \\ &\leq \exp\left(n \ln 2 - \frac{\varepsilon(1 - 2\theta^2)}{(1 - 2\theta^2 + 2\theta)} n \ln n\right) \rightarrow 0 \text{ при } n \rightarrow \infty. \end{aligned}$$

Доказательство того факта, что $I_2 \rightarrow 0$ при $n \rightarrow \infty$, аналогично соответствующему доказательству из теоремы 2. В итоге получаем неравенства

$$\mathcal{P} \geq 1 - I_1 - I_2 - I_3 \geq 2 - e^{-w_n},$$

что и требовалось доказать. Содержательность полученной оценки доказывается аналогично теореме 1. $\square$

Аналогично теоремам 1 и 2 доказывается следующая теорема.

Теорема 4. Пусть для заведомо совместной системы уравнений с искаженными правыми частями вида (4) выполняются условия: функции $h^{(i)}$, $i = \overline{1, t}$, принадлежат $[f_4]$ или $[f_5]$, $0 < \theta < 1$, $0 \leq p < 0.5$, $\delta = 1 - \sqrt{4p(1-p)}$ и

$$t = n(\ln n + w_n) / [4\theta(1-\theta)(2-\theta)\delta],$$

где $w_n = o(\ln n)$, $w_n > 2$, $n \rightarrow \infty$. Тогда при $n \rightarrow \infty$ вероятность правильного решения системы (4) методом максимального правдоподобия удовлетворяет неравенству

$$\mathcal{P} \geq 2 - e^{-w_n}.$$

Список литературы

- [1] Schaefer T., “Complexity of satisfiability problems”, Proc. 10 Annu. ACM Symp. Theory Comput. Mach., 1978, 216–226.
- [2] Горшков С.П., “Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений”, *Обозр. прикл. и промышл. матем.*, **2:3** (1995), 325–398.
- [3] Горшков С.П., Тарасов А.В., *Сложность решения систем булевых уравнений*, М.: Курс, 2017, 192 с.
- [4] Тарасов А.В., “О свойствах функций, представимых в виде 2-КНФ”, *Дискретная математика*, **13:4** (2001), 99–115.
- [5] Тарасов А.В., “Некоторые свойства групп инерции булевых бинюктивных функций и индуктивный метод генерации таких функций”, *Дискретная математика*, **14:2** (2002), 34–47.
- [6] Балакин Г.В., “Графы двучленных систем уравнений с булевыми неизвестными”, *Теория вероятн. и ее примен.*, **40:2** (1995), 241–259.
- [7] Балакин Г.В., Никольский Ю.Б., *Обозр. прикл. и промышл. матем.*, **2:3** (1995), 468–476.
- [8] Балакин Г.В., “Введение в теорию случайных систем уравнений”, Труды по дискретной математике, **1**, 1997, 1–18.
- [9] Балакин Г.В., “Системы случайных булевых уравнений со случайным выбором неизвестных в каждом уравнении”, Труды по дискретной математике, **3**, 2000, 21–28.

3. Приложение

Множества $\tilde{S}$ для дважды биюнктивных функций.

f_1 : 011 013 022 023 031 032 100 101 102 103 110 111 112 113 120 121 130
131 200 201 202 203 210 212 220 221 222 223 230 232

f_2 : 011 013 022 023 031 032 101 103 110 111 112 113 121 122 130 131 202
203 211 212 220 221 222 223 230 232 301 302 310 311 320 322

f_3 : 001 002 011 012 021 022 031 032 102 103 110 111 122 123 130 131 201
203 211 213 220 222 230 232 310 311 312 313 320 321 322 323

f_4 : 0011 0013 0022 0023 0031 0032 0111 0113 0122 0123 0131 0132 0211
0213 0222 0223 0231 0232 0311 0313 0322 0323 0331 0332 1011 1013 1022
1023 1031 1032 1100 1101 1102 1103 1110 1111 1112 1113 1120 1121 1130
1131 1211 1213 1222 1223 1231 1232 1300 1301 1302 1303 1310 1311 1312
1313 1320 1321 1330 1331 2011 2013 2022 2023 2031 2032 2111 2113 2122
2123 2131 2132 2200 2201 2202 2203 2210 2212 2220 2221 2222 2223 2230
2232 2300 2301 2302 2303 2310 2312 2320 2321 2322 2323 2330 2332 3011
3013 3022 3023 3031 3032 3100 3101 3102 3103 3110 3111 3112 3113 3120
3121 3130 3131 3200 3201 3202 3203 3210 3212 3220 3221 3222 3223 3230
3232

f_5 : 0011 0013 0022 0023 0031 0032 0111 0113 0122 0123 0131 0132 0211
0213 0222 0223 0231 0232 0311 0313 0322 0323 0331 0332 1010 1011 1012
1013 1022 1023 1030 1031 1100 1101 1102 1103 1110 1111 1112 1113 1120
1121 1130 1131 1210 1211 1212 1213 1222 1223 1230 1231 1300 1301 1302
1303 1310 1311 1312 1313 1320 1321 1330 1331 2011 2013 2020 2021 2022
2023 2030 2032 2111 2113 2120 2121 2122 2123 2130 2132 2200 2201 2202
2203 2210 2212 2220 2221 2222 2223 2230 2232 2300 2301 2302 2303 2310
2312 2320 2321 2322 2323 2330 2332 3010 3011 3012 3013 3020 3021 3022
3023 3100 3101 3102 3103 3110 3111 3112 3113 3200 3201 3202 3203 3220
3221 3222 3223