R. L. Dobrushin, S. I. Ortyukov, Lower Bound for the Redundancy of Self-correcting Arrangements of Unreliable Functional Elements, *Probl. Peredachi Inf.*, 1977, Volume 13, Issue 1, 82–89

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том XIII 1977 Вып. 1

УДК 621.391.1 :519.2

О НИЖНЕЙ ОЦЕНКЕ ДЛЯ ИЗБЫТОЧНОСТИ САМОКОРРЕКТИРУЮЩИХСЯ СХЕМ ИЗ НЕНАДЕЖНЫХ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Р. Л. Добрушин, С. И. Ортюков

Рассматриваются схемы из ненадежных функциональных элементов. Предполагается, что все элементы схемы ошибаются независимо друг от друга с вероятностью ε. Под избыточностью самокорректирующейся схемы, реализующей некоторую функцию, понимается отношение числа элементов — сложности самокорректирующейся схемы из ненадежных элементов к сложности схемы из надежных элементов, реализующей ту же функцию. Показано, что для некоторых функций избыточность реализующих их самокорректирующихся схем растет не медленнее, чем логарифм сложности схемы из надежных элементов.

§ 1. Введение

В работе рассматривается вопрос об избыточности самокорректирующихся схем из ненадежных функциональных элементов, реализующих булевы функции. Предполагается, что все элементы схемы ошибаются (выдают неправильный результат) независимо друг от друга и от значений поступивших на них сигналов с вероятностью ε. Этот вопрос был впервые рассмотрен фон Нейманом в известной работе [1], где показано, что для любой схемы-прототипа из надежных элементов можно построить самокорректирующуюся схему из ненадежных элементов, реализующую ту же булеву функцию, что и схема-прототип. В следующей статье авторов будет показано, что несколько уточняя построения фон Неймана, можно доказать, что избыточность самокорректирующейся схемы растет не быстрее, чем логарифм числа элементов схемы-прототипа. (Самим фон Нейманом эта оценка была доказана для схем с многократно дублированным выходом.) Возникает следующий вопрос. Является ли необходимым такой рост избыточности самокорректирующихся схем? Данная работа дает частичный ответ на этот вопрос. А именно показано, что по крайней мере для некоторых булевых функций логарифмический рост избыточности реализующих их самокорректирующихся схем является необходимым.

§ 2. Основные определения и формулировка результата

Рассмотрим направленный граф G. Пусть n_a — число всех ребер, идущих в вершину a графа G. Пусть $b_1(a), \ldots, b_{n_a}(a)$ — это ребра, идущие в вершину a из вершин $a_1(a), \ldots, a_{n_a}(a)$ соответственно. Вершины $a_1, a_2, \ldots, a_n$, в которые не идет ни одного ребра, называются входами графа G. Пусть задана некоторая совокупность вершин $\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_k$, из которых не идет ни одного ребра. Будем называть эти вершины выходами графа G. Пусть A — совокупность всех вершин графа G, а A_φ — совокупность всех вершин графа G, не являющихся входами. Пусть Φ — это некоторая полная система булевых функций.

Определение 2.1. Схемой S из функциональных элементов (или просто схемой) в базисе Φ называется конечный направленный граф G без циклов с фиксированной нумерацией его входов и выходов, а также ребер, идущих в каждую его вершину, каждой вершине $a\in A_\varphi$ которого сопоставлена булева функция $\varphi_a(x_1, \dots, x_{n_a})\in\Phi$, а каждому ребру $b_\rho(a)$, $\rho=1, \dots, n_a$, идущему в вершину a, сопоставлен аргумент x_ρ этой булевой функции.

Каждую вершину $a\in A_\varphi$ будем называть функциональным элементом, реализующим булеву функцию φ_a. Числом входов функционального элемента будем называть число ребер, идущих в вершину a, т. е. число n_a. Величину $L(S)$ — число функциональных элементов схемы S — будем называть сложностью схемы S.

Пусть X^n — это совокупность всех n-компонентных двоичных векторов $\mathbf{x}=(x_1, \dots, x_n)$, $x_i\in\{0, 1\}$, $i=1, 2, \dots, n$. Будем говорить, что двоичный вектор $\mathbf{z}=(z_1, z_2, \dots, z_n)$ — есть сумма по модулю два двоичных векторов $\mathbf{x}=(x_1, x_2, \dots, x_n)$ и $\mathbf{y}=(y_1, y_2, \dots, y_n)$ и писать $\mathbf{z}=\mathbf{x}\oplus\mathbf{y}$, если $z_i=x_i\oplus y_i$, $i=1, 2, \dots, n$, где символ $\oplus$ здесь и далее обозначает сложение по модулю два.

Фиксируем число $\varepsilon\in[0, 1/2)$. Пусть $\eta(a, \varepsilon)$, $a\in A_\varphi$ — это независимые случайные величины, принимающие значения 0 и 1, такие, что $\Pr\{\eta(a, \varepsilon)=1\}=\varepsilon$.

Определение 2.2. Под состоянием схемы S, соответствующим входному вектору $\mathbf{x}\in X^n$, при вероятности сбоев, равной ε, будем понимать систему случайных величин $\xi(a, \mathbf{x}, \varepsilon)$, $a\in A$, таких, что

1) $\xi(a_i, \mathbf{x}, \varepsilon)\equiv x_i$, $i=1, 2, \dots, n$,

2) $\xi(a, \mathbf{x}, \varepsilon)=\varphi_a(\boldsymbol{\xi}(a, \mathbf{x}, \varepsilon))\oplus\eta(a, \varepsilon)$, $a\in A_\varphi$,

где $\boldsymbol{\xi}(a, \mathbf{x}, \varepsilon)=(\xi(a_1(a), \mathbf{x}, \varepsilon), \dots, \xi(a_{n_a}(a), \mathbf{x}, \varepsilon))$.

Заметим, что поскольку схема S — это направленный граф без циклов, то определение 2.2 однозначно задает совместное распределение всех случайных величин $\xi(a, \mathbf{x}, \varepsilon)$.

Булевой k-мерной вектор-функцией от n переменных $\mathbf{f}(x_1, x_2, \dots, x_n)$ будем называть k-компонентный вектор, компонентами которого являются булевы функции от n переменных, т. е.

$$\mathbf{f}(x_1, x_2, \dots, x_n)=(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)), \tag{2.1}$$

где $f_j(x_1, \dots, x_n)$, $j=1, \dots, k$ — булевы функции от n переменных.

Определение 2.3. Будем говорить, что схема S реализует булеву k-мерную вектор-функцию $\mathbf{f}(\mathbf{x})$, $\mathbf{x}\in X^n$ с вероятностью ошибки $P(S, \mathbf{f})$ при вероятности сбоев, равной ε, если

$$P(S, \mathbf{f})=\max_{\mathbf{x}\in X^n}\left\{\frac{1}{k}\sum_{j=1}^{k}\Pr\{\xi(\tilde{a}_j, \mathbf{x}, \varepsilon)\neq f_j(\mathbf{x})\}\right\}. \tag{2.2}$$

Пусть $L_{p,\varepsilon}(\mathbf{f}, \Phi)$ — это минимальная сложность схемы в базисе Φ, реализующей булеву вектор-функцию $\mathbf{f}$ с вероятностью ошибки, не большей p, при вероятности сбоев, равной ε. Пусть $L(\mathbf{f}, \Phi)=L_{0,0}(\mathbf{f}, \Phi)$, т. е. $L(\mathbf{f}, \Phi)$ — минимальная сложность схемы из надежных функциональных элементов в базисе Φ, реализующей булеву вектор-функцию $\mathbf{f}$. Пусть

$$R_{p,\varepsilon}(\mathbf{f}, \Phi)=L_{p,\varepsilon}(\mathbf{f}, \Phi)/L(\mathbf{f}, \Phi). \tag{2.3}$$

Величину $R_{p,\varepsilon}(\mathbf{f}, \Phi)$ будем называть избыточностью минимальной схемы из ненадежных элементов в базисе Φ, реализующей булеву вектор-функцию $\mathbf{f}$ с вероятностью ошибки, не большей p, при вероятности сбоев, равной ε. Введем величину

$$R_{p,\varepsilon}(N, \Phi) = \max_{\mathbf{f}} R_{p,\varepsilon}(\mathbf{f}, \Phi), \tag{2.4}$$

где максимум берется по всем булевым вектор-функциям f таким, что $L(\mathbf{f}, \Phi) = N$. Основным результатом работы является следующая теорема.

Теорема 2.1. *Пусть* $p \in (0, 1/3)$, $\varepsilon \in (0, 1/2)$. *Тогда*

$$R_{p,\varepsilon}(N) \geqslant \frac{\ln\{((N/C(\Phi))-1)(n(\Phi)-1)(1-3p)p^{-1}\}}{C(\Phi)\ln\{n(\Phi)/\varepsilon\}} - \frac{1}{N}\left(\frac{\ln\{((N/C(\Phi))-1)(n(\Phi)-1)(1-3p)p^{-1}\}}{\ln\{n(\Phi)/\varepsilon\}} + \frac{1}{n(\Phi)-1}\right), \tag{2.5}$$

где $n(\Phi) = \max\limits_{\varphi \in \Phi} n(\varphi)$, *а* $n(\varphi)$ — *число переменных булевой функции* φ; $C(\Phi) = L(s, \Phi)$, *где булева функция* $s = s(x_1, \ldots, x_{n(\Phi)}) = x_1 \oplus \ldots \oplus x_{n(\Phi)}$, *т. е.* $C(\Phi)$ — *это минимальное число надежных функциональных элементов, необходимое для реализации двоичного сумматора* $n(\Phi)$ *чисел схемой в базисе* Φ.

Из формулы (2.5) видно, что при $N \to \infty$

$$R_{p,\varepsilon}(N) \gtrsim \frac{\ln N}{C(\Phi)\ln\{n(\Phi)/\varepsilon\}}. \tag{2.6}$$

§ 3. Вывод нижней оценки для избыточности

Введенное выше состояние схемы соответствует представлению о том, что ошибки в функциональных элементах происходят только на их выходах. При получении нижней оценки для избыточности нам удобно представлять себе, что ошибки в ненадежных элементах происходят не только на выходах, но и на входах. Ниже будет введено состояние схемы, соответствующее такому представлению о ненадежных элементах, причем это будет сделано так, чтобы не изменить вероятность ошибки схемы.

Рассмотрим произвольную схему S в базисе Φ. Пусть B — совокупность всех ребер схемы S. Пусть ζ_b, $b \in B$ и $\nu_a(\boldsymbol{\tau})$, $a \in A_\varphi$, $\boldsymbol{\tau} \in X^{n_a}$ — независимые случайные величины, принимающие значения 0 и 1, причем $\Pr\{\zeta_b = 1\} = \delta$, а $\Pr\{\nu_a(\boldsymbol{\tau}) = 1\} = P_a(\boldsymbol{\tau}, \delta)$, где $\delta \in [0, \varepsilon/n(\Phi)]$, а вероятности $P_a(\boldsymbol{\tau}, \delta)$ подобраны таким образом, что для любых $a \in A_\varphi$ и $\mathbf{t} \in X^{n_a}$

$$\Pr\{\varphi_a(\mathbf{t} \oplus \boldsymbol{\zeta}_a) \oplus \nu_a(\mathbf{t} \oplus \boldsymbol{\zeta}_a) \neq \varphi_a(\mathbf{t})\} = \varepsilon, \tag{3.1}$$

где $\boldsymbol{\zeta}_a = (\zeta_{b_1(a)}, \ldots, \zeta_{b_{n_a}(a)})$.

Лемма 3.1. *Пусть* $\varepsilon \in (0, 1/2)$, $\delta \in [0, \varepsilon/n(\Phi)]$. *Тогда для любой вершины* $a \in A_\varphi$ *существуют и единственны значения* $P_a(\boldsymbol{\tau}, \delta)$, $\boldsymbol{\tau} \in X^{n_a}$, *удовлетворяющие* (3.1.) *и такие, что* $P_a(\boldsymbol{\tau}, \delta) \in [0, 1]$.

Доказательство. При доказательстве вершину a будем полагать фиксированной и будем опускать индекс a у введенных выше величин. Применяя к (3.1) формулу полной вероятности и используя независимость случайных величин $\nu(\boldsymbol{\tau})$ и ζ_b, перепишем (3.1) в виде

$$\sum_{\boldsymbol{\tau} \in X^n} \Pr\{\nu(\boldsymbol{\tau}) \oplus \varphi(\boldsymbol{\tau}) \oplus \varphi(\mathbf{t}) = 1\} \Pr\{\boldsymbol{\zeta} = \mathbf{t} \oplus \boldsymbol{\tau}\} = \varepsilon, \mathbf{t} \in X^n. \tag{3.2}$$

Пусть

$$c(\mathbf{t}, \boldsymbol{\tau}, \delta) = (-1)^{\varphi(\boldsymbol{\tau}) \oplus \varphi(\mathbf{t})} \Pr\{\boldsymbol{\zeta} = \mathbf{t} \oplus \boldsymbol{\tau}\} = (-1)^{\varphi(\boldsymbol{\tau}) \oplus \varphi(\mathbf{t})} \delta^{w(\mathbf{t} \oplus \boldsymbol{\tau})} (1-\delta)^{n - w(\mathbf{t} \oplus \boldsymbol{\tau})}, \tag{3.3}$$

где $w(\mathbf{t})$, $\mathbf{t}\in X^n$ — это число единиц двоичного вектора $\mathbf{t}$. Перепишем соотношение (3.2) с учетом (3.3)

$$(3.4)\qquad \sum_{\tau\in X^n} P(\tau, \delta)\, c(\mathbf{t}, \tau, \delta) = \varepsilon + \sum_{\substack{\tau\in X^n\\ \tau:\varphi(\tau)\neq\varphi(\mathbf{t})}} c(\mathbf{t}, \tau, \delta),\ \mathbf{t}\in X^n.$$

Таким образом, для нахождения величин $P(\tau, \delta)$, $\tau\in X^n$ мы имеем систему из 2^n линейных уравнений с 2^n неизвестными.

Докажем теперь два утверждения относительно коэффициентов этой системы. А именно для всех $\mathbf{t}\in X^n$ при $\delta\in[0, \varepsilon / n(\Phi)]$

$$(3.5)\qquad \sum_{\tau\in X^n,\ \tau\neq \mathbf{t}} |c(\mathbf{t}, \tau, \delta)| < \varepsilon$$

и

$$(3.6)\qquad |c(\mathbf{t}, \mathbf{t}, \delta)| > 1-\varepsilon.$$

Действительно, заметим, что согласно (3.3)

$$(3.7)\qquad \sum_{\tau\in X^n} |c(\mathbf{t}, \tau, \delta)| = 1.$$

Тогда с учетом (3.3) имеем

$$\sum_{\tau\in X^n,\ \tau\neq \mathbf{t}} |c(\mathbf{t}, \tau, \delta)| = 1 - |c(\mathbf{t}, \mathbf{t}, \delta)| =$$
$$= 1-(1-\delta)^n \leqslant 1-(1-(\varepsilon/n(\Phi)))^{n(\Phi)} < \varepsilon.$$

Отсюда и из (3.7) следует (3.6).

Из (3.5) и (3.6) следует, что для матрицы коэффициентов системы (3.4) выполнено условие Адамара [2] (см. § 14.1). А именно для $\forall \mathbf{t}\in X^n$

$$(3.8)\qquad |c(\mathbf{t}, \mathbf{t}, \delta)| > \sum_{\tau\in X^n,\ \tau\neq \mathbf{t}} |c(\mathbf{t}, \tau, \delta)|.$$

При выполнении этого условия определитель системы не равен нулю. Следовательно, существует единственный набор величин $P(\tau, \delta)$, $\tau\in X^n$, удовлетворяющий (3.4).

Так как $c(\mathbf{t}, \tau, 0)=0$ при $\mathbf{t}\neq\tau$ и $c(\mathbf{t}, \mathbf{t}, 0)=1$, то $P(\tau, 0)=\varepsilon$, $\tau\in X^n$. Покажем, что при $\delta\in[0, \varepsilon/n(\Phi)]$ все величины $P(\tau, \delta)\in(0, 1)$. Предположим, что это не так. Тогда, поскольку $P(\tau, 0)=\varepsilon\in[0, 1]$ и $P(\tau, \delta)$ — это непрерывные функции от δ при $\delta\in[0, \varepsilon/n(\Phi)]$, то существуют $\tau'\in X^n$ и $\delta'\in[0, \varepsilon/n(\Phi)]$ такие, что либо $P(\tau', \delta']=0$ и $P(\tau, \delta')\in[0, 1]$, $\tau\in X^n$, либо $P(\tau', \delta')=1$ и $P(\tau, \delta')\in[0, 1]$, $\tau\in X^n$.

Рассмотрим первый случай. Из (3.4), положив $\mathbf{t}=\tau'$ и $\delta=\delta'$, получаем

$$(3.9)\qquad P(\tau', \delta')\, c(\tau', \tau', \delta') = \varepsilon + \sum_{\tau\in X^n,\ \tau:\varphi(\tau)\neq\varphi(\tau')} (1-P(\tau, \delta'))\times$$
$$\times\, c(\tau', \tau, \delta') - \sum_{\tau\in X^n,\ \tau:\varphi(\tau)=\varphi(\tau'),\ \tau\neq\tau'} P(\tau, \delta')\, c(\tau', \tau, \delta').$$

Так как $P(\tau, \delta')\in[0, 1]$, то из (3.9) и (3.5) следует, что

$$P(\tau', \delta'), c(\tau', \tau', \delta') \geqslant \varepsilon - \sum_{\tau\in X^n,\ \tau\neq\tau'} |c(\tau', \tau, \delta')| > 0.$$

Так как $c(\tau', \tau', \delta')>0$, то получаем противоречие с тем, что $P(\tau', \delta')=0$.

Во втором случае с учетом того, что $P(\tau, \delta')\in[0, 1]$, $c(\tau', \tau, \delta')\geqslant 0$ при $\varphi(\tau')=\varphi(\tau)$ и $c(\tau', \tau, \delta')\leqslant 0$ при $\varphi(\tau')\neq\varphi(\tau)$ из (3.9) получаем, что

$$(3.10)\qquad P(\tau', \delta')\, c(\tau', \tau', \delta') \leqslant \varepsilon.$$

Так как $c(\tau', \tau', \delta')>1-\varepsilon$ и $\varepsilon\in(0, 1/2)$, то из (3.10) следует, что $P(\tau', \delta')<\varepsilon/(1-\varepsilon)<1$. Полученное противоречие показывает, что $P(\tau, \delta)\in(0, 1)$, $\tau\in X^n$ при $\delta\in[0, \varepsilon/n(\Phi)]$. Лемма доказана.

Определение 3.1. Под θ-состоянием схемы S, соответствующим входному вектору $\mathbf{x}\in X^n$, при вероятности сбоев равной ε, будем понимать систему случайных величин $\theta(a, \mathrm{x}, \varepsilon)$, $a\in A$ таких, что

1) $\theta(a_i, \mathbf{x}, \varepsilon)\equiv x_i$, $i=1, 2, \ldots, n$,

2) $\theta(a, \mathrm{x}, \varepsilon)=\varphi_a(\boldsymbol{\theta}(a, \mathbf{x}, \varepsilon)\oplus\boldsymbol{\zeta}_a)\oplus\nu_a(\boldsymbol{\theta}(a, \mathrm{x}, \varepsilon)\oplus\boldsymbol{\zeta}_a)$, $a\equiv A_\varphi$,

где $\boldsymbol{\theta}(a, \mathrm{x}, \varepsilon)=(\theta(a_1(a), \mathbf{x}, \varepsilon), \ldots, \theta(a_{n_a}(a), \mathrm{x}, \varepsilon))$.

Таким образом, θ-состояние схемы соответствует следующему представлению о функционировании ненадежных элементов. Сигналы, пришедшие на входы элемента, искажаются независимо друг от друга с одинаковой вероятностью δ. Сигнал на выходе элемента искажается с вероятностью, зависящей от прошедших искажений входных сигналов таким образом, что вероятность того, что элемент выдаст неправильный результат, в точности равна ε. Следующая лемма показывает, что состояние и θ-состояние схемы эквивалентны в том смысле, что дают одинаковое значение для вероятности ошибки схемы.

Лемма 3.2. *Для любой схемы S в произвольном конечном базисе Φ при любых $\mathrm{x}\in X^n$, $\varepsilon\in(0, 1/2)$ и вершины $a\in A$*

(3.11) $$\Pr\{\theta(a, \mathrm{x}, \varepsilon)=1\}=\Pr\{\xi(a, \mathbf{x}, \varepsilon)=1\}.$$

Доказательство. Введем глубину $\Gamma(a)$ вершины a схемы S, под которой будем понимать максимальную длину пути от входов схемы до вершины a. Пусть $a^1, a^2, \ldots, a^{L(S)+n}$ — это совокупность всех вершин схемы S, пронумерованных некоторым образом в порядке неубывания глубины. Пусть $\xi_r=\xi(a^r, \mathbf{x}, \varepsilon)$, $\theta_r=\theta(a^r, \mathrm{x}, \varepsilon)$, $\boldsymbol{\xi}_r=(\xi_1, \xi_2, \ldots, \xi_r)$, а $\boldsymbol{\theta}_r=(\theta_1, \theta_2, \ldots, \theta_r)$, $r=1, 2, \ldots, L(S)+n$. Для произвольного двоичного вектора $\mathbf{z}=(z_1, z_2, \ldots, z_{L(S)+n})$ длины $L(S)+n$ пусть $\mathbf{z}^r=(z_1, z_2, \ldots, z_r)$.

Для доказательства леммы достаточно показать, что распределения вероятностей векторных случайных величин $\boldsymbol{\xi}_{L(S)+n}$ и $\boldsymbol{\theta}_{L(S)+n}$ совпадают, т. е., что для любого $\mathbf{z}\in X^{L(S)+n}$

(3.12) $$\Pr\{\boldsymbol{\xi}_{L(S)+n}=\mathbf{z}\}=\Pr\{\boldsymbol{\theta}_{L(S)+n}=\mathbf{z}\}.$$

Рассмотрим

(3.13) $$\Pr\{\boldsymbol{\xi}_{L(S)+n}=\mathbf{z}\}=\Pr\{\boldsymbol{\xi}_n=\mathbf{z}^n\}\Pr\{\xi_{n+1}=z_{n+1}\,|\,\boldsymbol{\xi}_n=\mathbf{z}^n\}\times \\ \times\Pr\{\xi_{n+2}=z_{n+2}\,|\,\boldsymbol{\xi}_{n+1}=\mathbf{z}^{n+1}\}\ldots\Pr\{\xi_{L(S)+n}=z_{L(S)+n}\,|\,\boldsymbol{\xi}_{L(S)+n-1}= \\ =\mathbf{z}^{L(S)+n-1}\}$$

и

(3.14) $$\Pr\{\boldsymbol{\theta}_{L(S)+n}=\mathbf{z}\}=\Pr\{\boldsymbol{\theta}_n=\mathbf{z}^n\}\Pr\{\theta_{n+1}=z_{n+1}\,|\,\boldsymbol{\theta}_n=\mathbf{z}^n\}\times \\ \ldots\times\Pr\{\theta_{L(S)+n}=z_{L(S)+n}\,|\,\boldsymbol{\theta}_{L(S)+n-1}=\mathbf{z}^{L(S)+n-1}\}.$$

Так как вершины $a^1, a^2, \ldots, a^n$ являются входами схемы S, то из определения состояния и θ-состояния схемы сразу следует, что

(3.15) $$\Pr\{\boldsymbol{\xi}_n=\mathbf{z}^n\}=\Pr\{\boldsymbol{\theta}_n=\mathbf{z}^n\}.$$

Таким образом, согласно (3.13), (3.14) и (3.15) для того, чтобы доказать (3.12), достаточно показать, что для любого $r=n+1, \ldots, n+L(S)$

(3.16) $$\Pr\{\xi_r=z_r\,|\,\boldsymbol{\xi}_{r-1}=\mathbf{z}^{r-1}\}=\Pr\{\theta_r=z_r\,|\,\boldsymbol{\theta}_{r-1}=\mathbf{z}^{r-1}\}.$$

Пусть в вершину a^r идут ребра из вершин $a^{r_\rho}=a_\rho(a^r)$, $\rho=1, 2, \ldots, n_a$. Так как $\Gamma(a^{r_\rho})\leqslant\Gamma(a^r)-1$, то $r_\rho<r$, $\rho=1, 2, \ldots, n_a$ и из определений состоя-

ния и θ-состояния схемы следует, что

(3.17) $$\Pr\{\xi_r=z_r|\xi_{r-1}=\mathbf{z}^{r-1}\}=\Pr\{\theta_r=z_r|\theta_{r-1}=\mathbf{z}^{r-1}\}= =\begin{cases}\varepsilon, \text{ если } z_r\neq\varphi_{a^r}(z_{r_1},\ldots,z_{r_{n_a}}),\\ 1-\varepsilon, \text{ если } z_r=\varphi_{a^r}(z_{r_1},\ldots,z_{r_{n_a}}).\end{cases}$$

Таким образом, соотношение (3.12), а вместе с ним и лемма доказаны.

В дальнейшем нам понадобится следующая вспомогательная лемма.

Лемма 3.3 *Пусть* $p\in(0,\ 1/3)$, $\delta\in(0,\ 1/2)$. *Пусть Q — произвольное множество натуральных чисел, число элементов которого $|Q|<\infty$, а m_l, $l\in Q$ — это некоторые целые неотрицательные числа. Пусть H_l, $l\in Q$ — это независимые события такие, что*

(3.18) $$\Pr\{H_l\}\geqslant\exp\{-m_l\ln(1/\delta)\},$$

(3.19) $$p\geqslant(1-p)\Pr\Big\{\widetilde{\bigcup_{l\in Q}}H_l\Big\},$$

где событие $\{\widetilde{\bigcup_{l\in Q}}H_l\}$ состоит в том, что произошло ровно одно из событий H_l, $l\in Q$, тогда

(3.20) $$\sum_{l\in Q}m_l\geqslant\frac{|Q|}{\ln(1/\delta)}\ln\left\{\frac{|Q|(1-3p)}{p}\right\}.$$

Доказательство. Сначала индукцией по мощности множества Q покажем, что для любого $\gamma\in(0,\ 1/2)$ из того, что $\Pr\{\widetilde{\bigcup_{l\in Q}}H_l\}\leqslant\gamma$, следует, что

(3.21) $$\Pr\Big\{\widetilde{\bigcup_{l\in Q}}H_l\Big\}\geqslant(1-2\gamma)\sum_{l\in Q}\Pr\{H_l\}.$$

Если $|Q|=1$, то неравенство (3.21) выполнено.

Предположим, что (3.21) выполнено для любого Q такого, что $|Q|=$ $=M$. Пусть $Q'=Q\cup l'$, где $l'\notin Q$. Тогда $|Q'|=|Q|+1=M+1$. Рассмотрим

$$\Pr\Big\{\widetilde{\bigcup_{l\in Q'}}H_l\Big\}=\Pr\Big\{\widetilde{\bigcup_{l\in Q}}H_l\Big\}+\Pr\{H_{l'}\}-$$
$$-2\Pr\Big\{\widetilde{\bigcup_{l\in Q}}H_l\Big\}\Pr\{H_{l'}\}\geqslant(1-2\gamma)\sum_{l\in Q'}\Pr\{H_l\}.$$

Таким образом, неравенство (3.21) доказано.

Из (3.19), (3.21) и (3.18) следует, что

(3.22) $$\Pr\Big\{\widetilde{\bigcup_{l\in Q'}}H_l\Big\}\geqslant\left(1-2\frac{p}{1-p}\right)\sum_{l\in Q}\Pr\{H_l\}\geqslant$$
$$\geqslant\frac{1-3p}{1-p}\sum_{l\in Q}\exp\left\{-m_l\ln\frac{1}{\delta}\right\}.$$

Применяя неравенство между средним арифметическим и средним геометрическим [3], из (3.19) и (3.22) получаем, что

$$p\geqslant(1-3p)|Q|\exp\left\{-\frac{\ln(1/\delta)}{|Q|}\sum_{l\in Q}m_l\right\}.$$

Логарифмируя это неравенство, получаем (3.20). Лемма 3.3 доказана.

Рассмотрим булеву k-мерную вектор-функцию $\mathbf{f}$ от n переменных. Фиксируем вектор $\mathbf{x}\in X^n$. Пусть $\mathbf{x}^l=(x_1^l,\ldots,x_n^l)$ — это двоичный вектор, отличающийся от $\mathbf{x}$ только l-й компонентой, т. е. $x_i^l=x_i$ при всех $i\neq l$ и $x_l^l=\bar{x}_l$. Пусть $Q_j(\mathbf{f},\ \mathbf{x})$, $j=1,\ 2,\ldots,\ k$ — это совокупность всех натуральных чисел $l\leqslant n$, таких, что $f_j(\mathbf{x})\neq f_j(\mathbf{x}^l)$. Пусть $W_j(\mathbf{f},\ \mathbf{x})=|Q_j(\mathbf{f},\ \mathbf{x})|$, т. е. величина $W_j(\mathbf{f}, \mathbf{x})$ — это число переменных булевой вектор-функции $\mathbf{f}$ таких, что при фиксированном векторе $\mathbf{x}$ изменение любого из этих переменных приводит к изменению значения j-й компоненты вектор-функции $\mathbf{f}$. Пусть

$$W(\mathbf{f}) = \max_{j=1,\dots,k} \max_{\mathbf{x}\in X^n} W_j(\mathbf{f}, \mathbf{x}). \tag{3.23}$$

Теорема 3.1. *Пусть S — это минимальная по сложности схема в базисе Φ, реализующая булеву k-мерную вектор-функцию $\mathbf{f}$ с вероятностью ошибки, не большей $p\in(0, 1/3)$, при вероятности сбоев $\varepsilon\in(0, 1/2)$. Тогда*

$$L(S) \geqslant \frac{W(\mathbf{f})\ln\{W(\mathbf{f})(1-3p)p^{-1}\}}{(n(\Phi)-1)\ln\{n(\Phi)/\varepsilon\}} - \frac{k}{n(\Phi)-1} \tag{3.24}$$

Доказательство. Пусть максимум в (3.23) достигается при $j=j_0$ и $\mathbf{x}=\mathbf{x}_0$. Введем события E и E_l, положив $E=\{\theta(\tilde{a}_{j_0}, \mathbf{x}_0, \varepsilon)\neq f_{j_0}(\mathbf{x}_0)\}$, $E_l=\{\theta(\tilde{a}_{j_0}, \mathbf{x}_0^l, \varepsilon)=f_{j_0}(\mathbf{x}_0^l)\}$. Пусть B_l, $l=1,\dots, n$ — это совокупность всех ребер, идущих из входа a_l схемы S. Для любого множества $\beta\subset B_l$ введем событие

$$H_l(\beta)=\{(\zeta_b=1, \text{ если } b\in\beta)\cap(\zeta_b=0, \text{ если } b\in B_l\setminus\beta)\}.$$

Пусть множество $\beta_l\subset B_l$ таково, что

$$\Pr\{E_l | H_l(\beta_l)\} = \max_{\beta\subset B_l} \Pr\{E_l | H_l(\beta)\}. \tag{3.25}$$

Введем обозначения $H_l=H_l(B_l\setminus\beta_l)$ и $\tilde{H}_l=H_l(\beta_l)$. Тогда

$$\Pr\{E\}\geqslant\Pr\{E | \tilde{\bigcup_{l\in Q}} H_l\}\Pr\{\tilde{\bigcup_{l\in Q}} H_l\}, \tag{3.26}$$

где $Q\equiv Q_{j_0}(\mathbf{f}, \mathbf{x}_0)$. Из леммы 3.2 и условия теоремы следует, что

$$\Pr\{E\}\leqslant p;\ \Pr\{E_l\}\geqslant 1-p. \tag{3.27}$$

Из определения θ-состояния схемы следует, что для всех $l\in Q$

$$\Pr\{E | H_l\}=\Pr\{E_l | \tilde{H}_l\}. \tag{3.28}$$

Согласно (3.25) и (3.27)

$$\Pr\{E_l | \tilde{H}_l\}\geqslant\Pr\{E_l\}\geqslant 1-p. \tag{3.29}$$

Из (3.29) и (3.28) следует, что

$$\Pr\{E | \tilde{\bigcup_{l\in Q}} H_l\}\geqslant 1-p. \tag{3.30}$$

Тогда из (3.26), (3.27) и (3.30) получаем

$$p\geqslant(1-p)\Pr\{\tilde{\bigcup_{l\in Q}} H_l\}. \tag{3.31}$$

Из независимости случайных величин ζ_b следует, что события H_l независимы. Заметим, что

$$\Pr\{H_l\}\geqslant\exp\{-|B_l|\ln(1/\delta)\}. \tag{3.32}$$

Сравнивая (3.31) и (3.19), (3.32) и (3.18), видим, что выполнены условия леммы 3.3 при $m_l=|B_l|$. С помощью результата этой леммы получаем

$$\sum_{l\in Q}|B_l|\geqslant\frac{|Q|}{\ln(1/\delta)}\ln\{|Q|(1-3p)p^{-1}\}. \tag{3.33}$$

Если из входов схемы S в базисе Φ идет N_B ребер, а N_A — это число вершин, из которых не идет ни одного ребра, то

(3.34) $$N_A \geqslant N_B - (n(\Phi)-1)L(S).$$

В минимальной схеме все вершины, из которых не идет ни одного ребра, являются выходами схемы. Так как схема S минимальна и $N_B \geqslant \sum_{l \in Q} |B_l|$, то с учетом (3.33) и (3.34) имеем

(3.35) $$k \geqslant \frac{|Q|}{\ln(1/\delta)} \ln\{|Q|(1-3p)p^{-1}\} - (n(\Phi)-1)L(S).$$

Так как $|Q| = W(\mathrm{f})$, то, положив $\delta = \varepsilon / n(\Phi)$, из (3.35) получаем (3.24). Теорема 3.1 доказана.

Доказательство теоремы 2.1. Рассмотрим одномерную булеву вектор-функцию $\tilde{f}(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$. Пусть $N = L(\tilde{f}, \Phi)$. Если в базис Φ входит булева функция $s = s(x_1, \ldots, x_{n(\Phi)}) = x_1 \oplus \ldots \oplus x_{n(\Phi)}$, то, построив схему S, реализующую функцию $\tilde{f}$, из надежных элементов, реализующих функцию s, в виде дерева, получим

(3.36) $$L(S) \leqslant (n-1)/(n(\Phi)-1)+1.$$

Тогда в случае произвольного базиса

(3.37) $$L(\tilde{f}, \Phi) = N \leqslant C(\Phi) L(S) \leqslant C(\Phi)((n-1)/(n(\Phi)-1)+1).$$

Отсюда

(3.38) $$n \geqslant (N/C(\Phi)-1)(n(\Phi)-1).$$

Пусть схема $\tilde{S}$ — это минимальная по сложности схема в базисе Φ, реализующая функцию $\tilde{f}$ с вероятностью ошибки не большей p, при вероятности сбоев, равной ε. Так как $W(\tilde{f}) = n$, то, используя результат теоремы 3.1, получаем

(3.39) $$L(\tilde{S}) \geqslant \frac{n \ln\{n(1-3p)p^{-1}\}}{(n(\Phi)-1)\ln\{n(\Phi)/\varepsilon\}} - \frac{1}{n(\Phi)-1}.$$

Согласно определению избыточности (2.4),

(3.40) $$R_{p,\varepsilon}(N) \geqslant L(\tilde{S})/N.$$

Из (3.38) – (3.40) следует (2.5).

Теорема доказана.

Авторы благодарны В. И. Левенштейну за ценные советы по содержанию этой статьи.

ЛИТЕРАТУРА

1. *Фон Нейман Дж.* Автоматы. М., Изд-во иностр. лит-ры, 1956.
2. *Гантмахер Ф. Р.* Теория матриц. М., «Наука», 1967.
3. *Беккенбах Э., Беллман Р.* Неравенства. М., «Мир», 1965.

Поступила в редакцию
9 января 1976 г.