Math-Net.Ru

Общероссийский математический портал

М. А. Алехина, А. В. Васин, О базисах с коэффициентом ненадежности 2, *Матем. заметки*, 2014, том 95, выпуск 2, 170–201

DOI: <https://doi.org/10.4213/mzm8784>

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: 52.205.19.152

26 апреля 2023 г., 11:06:40

О базисах с коэффициентом ненадежности 2

М. А. Алехина, А. В. Васин

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном базисе $B \subset B_3$ (B_3 – множество всех булевых функций, зависящих от переменных x_1, x_2, x_3). Предполагается, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах. В B_3 найдены все полные базисы, в которых выполняются два условия одновременно: 1) любую функцию можно реализовать схемой с ненадежностью, асимптотически не больше 2ε ($\varepsilon \rightarrow 0$); 2) существуют функции (обозначим их множество через K), которые нельзя реализовать схемами с ненадежностью, асимптотически меньше чем 2ε , $\varepsilon \rightarrow 0$. Такие базисы будем называть базисами с коэффициентом ненадежности 2. Доказано также, что множество K содержит почти все функции.

Библиография: 18 названий.

DOI: 10.4213/mzm8784

1. Введение, основные понятия и определения. Рассматривается реализация булевых функций схемами (определение схемы, полюса, вершины см., например, в книге [1]) из ненадежных функциональных элементов в полном конечном базисе B . Считаем, что схема S из ненадежных элементов *реализует* булеву функцию $f(x_1, \dots, x_n)$ (обозначим $\tilde{x} = (x_1, \dots, x_n)$), если при поступлении на входы схемы двоичного набора $\tilde{a}$ при отсутствии неисправностей на выходе схемы S появляется значение $f(\tilde{a})$.

Впервые задачу синтеза надежных схем из ненадежных функциональных элементов рассматривал фон Нейман [2]. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε , $\varepsilon \in (0; 1/2)$, подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию φ , а в неисправном – функцию $\bar{\varphi}$. С помощью итерационного метода фон Нейман установил, что в произвольном полном конечном базисе любую булеву функцию можно реализовать схемой, вероятность ошибки на выходе которой при любом входном наборе значений переменных не превосходит $c\varepsilon$ (c – некоторая константа, зависящая от базиса) при $\varepsilon \in (0; 1/6]$.

Схема из ненадежных элементов характеризуется двумя важными параметрами: вероятностью ошибки на выходе схемы и сложностью схемы. Основным недостатком метода фон Неймана состоит в том, что с ростом числа итераций сложность схем

увеличивается экспоненциально (примерно в 3^k раз, где k – число итераций). Поэтому именно сложности уделялось главное внимание в дальнейших исследованиях (см. работы Ортюкова [3], Улига [4], Яблонского [5]).

В этой статье, в отличие от упомянутых работ, сложность схем не рассматривается, а в центре нашего внимания будет максимальная вероятность ошибки на выходе схемы, которая реализует функцию “почти” наилучшим образом с точки зрения вероятности ошибки. В работе будут описаны базисы, в которых почти все функции можно реализовать схемами, максимальная вероятность ошибки на выходе которых асимптотически равна 2ε при $\varepsilon \rightarrow 0$.

Введем необходимые определения и понятия.

Ненадежностью $P(S)$ схемы S назовем максимальную вероятность ошибки на выходе схемы S при всевозможных входных наборах схемы. *Надежностью* схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим булеву функцию f . Схема A из ненадежных элементов, реализующая функцию f , называется *асимптотически оптимальной* (асимптотически наилучшей) по надежности, если

$$P(A) \sim P_\varepsilon(f) \quad \text{при} \quad \varepsilon \rightarrow 0, \quad \text{т.е.} \quad \lim_{\varepsilon \rightarrow 0} \frac{P_\varepsilon(f)}{P(A)} = 1.$$

Задачу построения асимптотически оптимальных по надежности схем в полных базисах из двухвходовых элементов решали: Алехина [6] при условии, что элементы схемы подвержены однотипным константным неисправностям только на входах или только на выходах элементов; Чугунова [7] при условии, что элементы схемы подвержены инверсным неисправностям на входах элементов.

Мы, так же, как и фон Нейман, будем считать, что базисные элементы подвержены инверсным неисправностям на выходах.

Число k будем называть *коэффициентом ненадежности базиса*, если выполняются два условия одновременно:

- 1) все функции в этом базисе можно реализовать схемами с ненадежностью, асимптотически не больше $k\varepsilon$, $\varepsilon \rightarrow 0$;
- 2) найдется функция, которую нельзя реализовать схемой с ненадежностью, асимптотически меньше чем $k\varepsilon$, $\varepsilon \rightarrow 0$.

Пусть k – коэффициент ненадежности базиса B . Обозначим через K (возможно, с нижними индексами) множество функций, для которых асимптотически оптимальные по надежности схемы в базисе B функционируют с ненадежностью, асимптотически равной $k\varepsilon$, $\varepsilon \rightarrow 0$.

Поясним, какие значения может принимать коэффициент ненадежности базиса.

Нетрудно проверить, что при инверсных неисправностях на выходах элементов в любом базисе ненадежность любой схемы, содержащей хотя бы один элемент, не меньше ε . Поэтому коэффициент ненадежности любого базиса не меньше 1.

Из результата фон Неймана [2] следует, что если базис содержит медиану (функцию голосования) $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$, то его коэффициент ненадежности равен 1. Оказалось, что существуют и другие базисы (не содержащие медиану), коэффициент ненадежности которых также равен 1 (некоторые из этих базисов приведем далее).

Аксенов [8] доказал, что в произвольном полном конечном базисе B любую функцию можно реализовать такой схемой S , что ее ненадежность

$$P(S) \leq 5\varepsilon + d\varepsilon^2 \quad (1)$$

при любом $\varepsilon \in (0, \varepsilon_0]$, где $d = 10584$, $\varepsilon_0 = 1/3600$.

Из этого результата следует, что коэффициент ненадежности любого полного конечного базиса не больше 5.

Позднее авторам [9] удалось ослабить ограничение на ε , а константу d уменьшить. Например, в качестве констант ε_0 , d можно взять $1/960$ и 182 соответственно. Далее этот результат сформулирован в виде теоремы 1.

Отрицательный ответ на вопрос о возможности снижения мультипликативной константы 5 в оценке ненадежности (1) для базиса $\{x_1x_2, \bar{x}_1\}$ получен Васиным в работе [10].

Таким образом, коэффициент ненадежности любого базиса принимает значения из отрезка $[1; 5]$.

Пусть S – любая схема в базисе B , содержащая хотя бы один функциональный элемент, а N – число элементов в ней, $N \in \mathbb{N}$. Тогда, применяя формулу полной вероятности, ненадежность $P(S)$ схемы S при всех $\varepsilon \in (0, 1/2)$ можно представить полиномом

$$P(S) = \sum_{i=1}^N c_i \varepsilon^i (1 - \varepsilon)^{n-i} \quad (2)$$

с целыми коэффициентами

$$c_1 \in \{1, 2, \dots, N\}, \quad c_i \in \left\{0, 1, \dots, \frac{N!}{i!(N-i)!}\right\}, \quad i = 2, 3, \dots, N.$$

Следовательно, $P(S) \sim c_1\varepsilon$ при $\varepsilon \rightarrow 0$. Учитывая, что коэффициент ненадежности любого базиса принимает значения из отрезка $[1; 5]$, получаем следующее утверждение.

УТВЕРЖДЕНИЕ 1. Коэффициент ненадежности любого полного конечного базиса принимает значения из множества $\{1, 2, 3, 4, 5\}$.

Итак, если в полном конечном базисе B каждая булева функция f реализована асимптотически оптимальной по надежности схемой S , функционирующей с ненадежностью $P(S) \sim c_f\varepsilon$, $c_f \in \{1, 2, 3, 4, 5\}$, при $\varepsilon \rightarrow 0$, то число $k = \max_{f \in P_2} c_f$ есть коэффициент ненадежности базиса B , а K – множество таких булевых функций f , что $c_f = k$.

Чтобы сформулировать ранее известные результаты о базисах с коэффициентом ненадежности 1, введем следующие понятия и множества.

Булевы функции f_1 и f_2 назовем *конгруэнтными*, если одна из них может быть получена из другой заменой переменных (без отождествления).

Пусть $f(\tilde{x})$ – произвольная булева функция. Набор $\tilde{a}$ такой, что $f(\tilde{a}) = 1$, будем называть *единичным* набором функции $f(\tilde{x})$. Набор $\tilde{a}$ такой, что $f(\tilde{a}) = 0$, будем называть *нулевым* набором функции $f(\tilde{x})$. Обозначим через N_f множество всех единичных наборов функции f .

Пусть $D \subseteq P_2$. Через D^* обозначим множество булевых функций, двойственных функциям множества D .

Пусть G_1 – множество функций, зависящих от переменных x_1, x_2, x_3 , каждая из которых конгруэнтна некоторой функции вида

$$x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3\}.$$

Пусть G_2 – множество функций, зависящих от переменных x_1, x_2, x_3 , каждая из которых конгруэнтна некоторой функции вида

$$x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3\}.$$

Пусть G_3 – множество функций, зависящих от переменных x_1, x_2, x_3 , каждая из которых конгруэнтна некоторой функции вида

$$x_1^{\sigma_1} x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3\}.$$

Нетрудно проверить, что $G_i^* = G_i$ $i = 1, 2, 3$. Полагаем $G = G_1 \cup G_2 \cup G_3$.

Изобразим на трехмерном булевом кубе множества N_{g_i} , $i = 1, 2, 3$, единичных наборов функций $g_i \in G_i$, например, в случае $\sigma_1 = \sigma_2 = \sigma_3 = 1$. Подставим эти значения в соответствующие выражения для функций множеств G_i . Тогда

$$g_1(x_1, x_2, x_3) = x_1 x_2 \vee x_1 x_3 \vee x_2 x_3 \in G_1,$$

$$g_2(x_1, x_2, x_3) = x_1 x_2 \oplus x_3 \in G_2,$$

$$g_3(x_1, x_2, x_3) = x_1 \bar{x}_2 \vee x_2 x_3 \in G_3.$$

На рис. 1 представлены изображения трехмерного куба, на которых темными точками отмечены множества N_{g_1} (см. рис. 1, а), N_{g_2} (см. рис. 1, б), N_{g_3} (см. рис. 1, в).

Рис. 1. Функции из G_1, G_2, G_3 при $(\sigma_1, \sigma_2, \sigma_3) = (1, 1, 1)$

Пусть G_4 – множество функций, зависящих от x_1, x_2, x_3, x_4 и конгруэнтных одной из функций вида

$$(x_1^{\sigma_1} x_2^{\sigma_2} \vee x_3^{\sigma_3} x_4^{\sigma_4})^{\sigma_5}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3, 4, 5\}.$$

Нетрудно проверить, что $G_4^* = G_4$.

Аксенов [8] доказал, что если полный базис B содержит хотя бы одну из функций множества $G_1 \cup G_4$ (т.е. $B \cap (G_1 \cup G_4) \neq \emptyset$), то его коэффициент ненадежности равен 1.

Обозначим B_i , $i \geq 2$, – множество всех булевых функций, зависящих от i переменных $x_1, \dots, x_i$. Ясно, что $\{\bar{x}_1, x_1, 0, 1\} \subset B_2 \subset B_3 \subset B_4$.

Доказано [9], что полный базис $B \subseteq B_3$ имеет коэффициент ненадежности 1 тогда и только тогда, когда $B \cap G \neq \emptyset$. Другими словами, множество G является критерияльным в том случае, когда нужно выяснить, равен ли 1 коэффициент ненадежности базиса $B \subseteq B_3$. Известно также [12], что множество G_4 таким свойством не обладает, т.е. среди полных базисов $B \subseteq B_4 \setminus (G \cup G_4)$ есть базисы с коэффициентом ненадежности 1.

В этой статье найдены все полные базисы B , $B \subseteq B_3$, для которых коэффициент ненадежности равен 2, а также показано, что класс K содержит почти все булевы функции. Чтобы сформулировать полученные результаты в виде теоремы, введем еще некоторые обозначения и множества.

Пусть $X \subseteq B_3$. Обозначим $\text{Congr}(X)$ – множество всех функций, зависящих от переменных x_1, x_2, x_3 , каждая из которых конгруэнтна некоторой функции множества X . Например,

$$\begin{aligned}\text{Congr}\{1, x_1, x_1 \& x_2\} &= \{1, x_1, x_2, x_3, x_1 \& x_2, x_2 \& x_3, x_1 \& x_3\}, \\ \text{Congr}\{\bar{x}_1, x_1, 0, 1\} &= \{\bar{x}_1, \bar{x}_2, \bar{x}_3, x_1, x_2, x_3, 0, 1\}.\end{aligned}$$

Введем следующие множества:

- 1) $M_1 = \text{Congr}\{x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}$, $|M_1| = 24$;
- 2) $M_2 = \text{Congr}\{x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\sigma_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} \vee x_1^{\bar{\sigma}_1} x_2^{\sigma_2} x_3^{\bar{\sigma}_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}$ и $|M_2| = 8$;
- 3) $M_3 = \text{Congr}\{\bar{x}_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}) \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}$, $|M_3| = 12$;
- 4) $M_4 = \text{Congr}\{x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}$, $|M_4| = 4$;
- 5) M_i^* – множество функций, двойственных соответственно функциям множества M_i , $i = 1, 2, 3, 4$;
- 6) $M = \bigcup_{i=1}^4 (M_i \cup M_i^*)$, $|M| = 96$, $|G \cup M| = 152$;
- 7) $M_5 = \text{Congr}\{x_1 \oplus x_2 \oplus a, x_1 \oplus x_2 \oplus x_3 \oplus b \mid a, b \in \{0, 1\}\}$, т.е. M_5 – множество линейных функций, существенно зависящих от двух или трех переменных; $|M_5| = 8$;
- 8) $\Theta = \text{Congr}\{x_1^{\sigma_1} x_2^{\sigma_2}, x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3}, x_1^{\sigma_1} (x_2^{\sigma_2} x_3^{\sigma_3} \vee x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3}) \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}$, $|\Theta| = 32$;
- 9) Θ^* – множество функций, двойственных функциям множества Θ ;
- 10) $\Psi = \Theta \cup \text{Congr}\{x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}) \mid \sigma_i \in \{0, 1\}, i \in \{2, 3\}\}$, $|\Psi| = 44$;
- 11) Ψ^* – множество функций, двойственных функциям множества Ψ , $|\Psi^*| = 44$;
- 12) $\tilde{\Psi} = \Psi \cup \Psi^* \cup \text{Congr}\{\bar{x}_1, x_1, 0, 1\}$, $|\tilde{\Psi}| = 96$; очевидно, что $\tilde{\Psi} = B_3 \setminus (G \cup M \cup M_5)$.

Мощности введенных множеств легко вычисляются непосредственным подсчетом.

Изобразим на трехмерном булевом кубе множества N_{h_i} , $i = 1, 2, 3, 4$, единичных наборов функций $h_i \in M_i$, например, в случае $\sigma_1 = \sigma_2 = \sigma_3 = 1$. Подставим эти

значения в соответствующие выражения для функций множеств M_i . Тогда

$$h_1(x_1, x_2, x_3) = x_1 x_2 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3 \in M_1,$$

$$h_2(x_1, x_2, x_3) = x_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 \bar{x}_3 \in M_2,$$

$$h_3(x_1, x_2, x_3) = \bar{x}_1 x_2 \vee x_3 \in M_3,$$

$$h_4(x_1, x_2, x_3) = x_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3 \in M_4.$$

На рис. 2 представлены изображения трехмерного куба, на которых темными точками отмечены множества N_{h_1} (см. рис. 2, а), N_{h_2} (см. рис. 2, б), N_{h_3} (см. рис. 2, в), N_{h_4} (см. рис. 2, д).

Рис. 2. Функции из M_1, M_2, M_3, M_4 при $(\sigma_1, \sigma_2, \sigma_3) = (1, 1, 1)$

Сформулируем в виде теоремы основной результат этой статьи.

ТЕОРЕМА 0. Пусть полный базис $B \subseteq B_3$. Коэффициент ненадежности базиса B равен 2 тогда и только тогда, когда $B \cap G = \emptyset$ и выполнено хотя бы одно из следующих условий:

- 1) $B \cap (M \cup M_5) \neq \emptyset$;
- 2) базис B содержит функцию $\varphi(x_1, x_2, x_3)$, конгруэнтную функции вида

$$x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}), \quad \sigma_2, \sigma_3 \in \{0, 1\},$$

$$\text{и } B \cap \Psi^* \neq \emptyset;$$

- 3) базис B содержит функцию $\varphi^*(x_1, x_2, x_3)$, конгруэнтную функции вида

$$x_1 \vee x_2^{\sigma_2} x_3^{\sigma_3},$$

$$\text{и } B \cap \Psi \neq \emptyset.$$

Кратко, без доказательств результаты этой теоремы сформулированы в работах [15], [16]. Кроме того, в работе [17] доказана теорема, аналогичная теореме 9 (отличие в коэффициенте при ε^2 , его удалось понизить с 200 до 65). Подробные и полные доказательства изложены в кандидатской диссертации Васина [18].

В следующем пункте в виде теорем и лемм сформулированы ранее известные результаты, которые будем использовать при доказательстве теоремы 0.

2. Ранее известные результаты. Напомним, что B – произвольный полный конечный базис.

Мы, так же, как и фон Нейман, для повышения надежности схем будем использовать итерационные методы, а в качестве исходных схем будем брать схемы из теоремы 1.

ТЕОРЕМА 1 [9]. В произвольном полном конечном базисе B любую функцию f можно реализовать такой схемой A , что

$$P(A) \leq 5\varepsilon + 182\varepsilon^2 \leq 5.2\varepsilon \quad \text{при всех } \varepsilon \in \left(0, \frac{1}{960}\right].$$

Пусть функция $g \in G_1$, т.е.

$$g(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3\}.$$

Наборы $(\sigma_1, \sigma_2, \sigma_3)$, $(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3)$ будем называть *характеристическими* наборами функции $g(x_1, x_2, x_3)$.

Например, если $g(x_1, x_2, x_3) = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_2 x_3$, то наборы $(0, 1, 1)$ и $(1, 0, 0)$ являются характеристическими наборами функции g .

Пусть функция $g \in G_4$, т.е.

$$g(x_1, x_2, x_3, x_4) = x_1^{\sigma_1} x_2^{\sigma_2} \vee x_3^{\sigma_3} x_4^{\sigma_4}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3, 4\},$$

или

$$g(x_1, x_2, x_3, x_4) = (x_1^{\sigma_1} \vee x_2^{\sigma_2})(x_3^{\sigma_3} \vee x_4^{\sigma_4}), \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3, 4\}.$$

Наборы $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$, $(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4)$ будем также называть *характеристическими* наборами функции $g(x_1, x_2, x_3, x_4)$.

Для повышения надежности исходных схем и получения верхних оценок ненадежности схем будем использовать схемы из теоремы 2 и леммы 1.

ТЕОРЕМА 2 [6]. Допустим, что любую функцию f в базисе B можно реализовать схемой с ненадежностью не больше p , $p \leq 1/2$. Пусть схема S_g реализует функцию $g \in (G_1 \cup G_4)$ с ненадежностью $P(S_g)$, причем v^1 и v^0 – вероятности ошибок схемы S_g на характеристических наборах. Тогда функцию f можно реализовать такой схемой S , что

$$\begin{aligned} P(S) &\leq \max\{v^0, v^1\} + 3pP(S_g) + 3p^2, & \text{если } g \in G_1, \\ P(S) &\leq \max\{v^0, v^1\} + 4pP(S_g) + 6p^2, & \text{если } g \in G_4. \end{aligned}$$

Обозначим через $N(S)$ число элементов схемы S .

ЛЕММА 1 [8]. Допустим, что в базисе B любую функцию f можно реализовать схемой с ненадежностью не больше p , $p \leq 1/2$. Пусть схема S_g содержит $N(S_g)$ элементов и реализует функцию $g \in (G_1 \cup G_4)$. Тогда функцию f можно реализовать такой схемой S , что

$$P(S) \leq \varepsilon N(S_g) + 6p^2.$$

Лемма 2 и теорема 3, приведенные ниже, используются для доказательства теоремы 9.

ЛЕММА 2 [13]. Пусть $\psi(x_1, x_2, \dots, x_m)$ – нелинейная функция, $m \geq 2$. Тогда из функции $\psi(x_1, x_2, \dots, x_m)$ подстановкой переменных можно получить функцию

$$\varphi_1(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$$

или

$$\varphi_2(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0,$$

где $a_0, a_1, a_2, a_3 \in \{0, 1\}$.

ТЕОРЕМА 3 [9]. Пусть базис B содержит функцию $g \in G_1$. Тогда любую функцию f в этом базисе можно реализовать схемой A с ненадежностью

$$P(A) \leq \varepsilon + 8\varepsilon^2$$

при всех $\varepsilon \in (0, 1/960]$.

В частности, если базис содержит функцию голосования

$$g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3 \in G_1,$$

то результат теоремы 3 в несколько ином виде получен фон Нейманом [2].

Следующие определение и теорема используются для того, чтобы результаты, полученные для базиса B , перенести в двойственный базис B^* .

Пусть E – функциональный элемент с функцией $e(x_1, x_2, \dots, x_r)$, $r \in \mathbb{N}$. Элемент E^* с функцией $e^*(x_1, x_2, \dots, x_r)$, двойственной функции $e(x_1, x_2, \dots, x_r)$, называется *двойственным* элементу E . Схему S^* назовем *двойственной* схеме S , если она получается из схемы S заменой всех элементов на двойственные им элементы соответственно.

ТЕОРЕМА 4 [14]. Ненадежности двойственных схем S и S^* равны, т.е. верно равенство $P(S) = P(S^*)$.

Пусть схема $S^{(1)}$ реализует систему булевых функций

$$f_1(x_1, \dots, x_n), \quad \dots, \quad f_k(x_1, \dots, x_n),$$

схема $S^{(2)}$ реализует булеву функцию $h(y_1, \dots, y_m)$ и схемы $S^{(1)}$ и $S^{(2)}$ не имеют общих вершин. При присоединении каждого i -го входа схемы $S^{(2)}$ к некоторому (одному) $\nu(i)$ -му выходу схемы $S^{(1)}$ и стирания переменных, приписанных входам схемы $S^{(2)}$ (см. рис. 3), получается схема (обозначим ее через S), реализующая функцию

$$h'(x_1, \dots, x_n) = h(f_{\nu(1)}(x_1, \dots, x_n), \dots, f_{\nu(m)}(x_1, \dots, x_n)).$$

Пусть S – произвольная схема. Схему $S^{(2)}$ (см. рис. 3) как с переменными $y_1, \dots, y_m$, приписанными ее входам, так и без них, будем называть *подсхемой* схемы S .

Очевидно, что вероятности ошибок на выходе схемы не изменятся при переименовании переменных (без отождествления), приписанных входам схемы. Поэтому при

Рис. 3

вычислении вероятностей ошибок на выходе подсхемы можно не указывать входные переменные подсхемы.

Например, функциональный элемент, выход которого является выходом схемы, есть подсхема.

Для получения нижних оценок ненадежности схем будем использовать следующую теорему из работы [6].

ТЕОРЕМА 5 [6]. Пусть $f(\tilde{x})$ – произвольная булева функция, отличная от константы, S – любая схема, ее реализующая. Пусть подсхема C схемы S содержит выход схемы S и реализует булеву функцию $h(y_1, \dots, y_m)$, $m \in \mathbb{N}$, с ненадежностью $P(C) \leq 1/2$. Обозначим через $p_{11}, \dots, p_{1r}$ всевозможные различные вероятности ошибок на выходе схемы C при нулевых входных наборах функции h . Аналогично, пусть $p_{01}, \dots, p_{0t}$ – всевозможные различные вероятности ошибок на выходе схемы C при единичных входных наборах функции h . Полагаем

$$p^1 = \min\{p_{11}, \dots, p_{1r}\}, \quad p^0 = \min\{p_{01}, \dots, p_{0t}\}.$$

Тогда

$$P(S) \geq \max\{p^0, p^1\}.$$

Пусть в схеме S , реализующей булеву функцию, отличную от константы, выделена подсхема A , имеющая один вход. Обозначим через S' схему, получаемую из схемы S удалением подсхемы A . Если выполнено неравенство $P(S) > P(S')$, то будем говорить, что схема S' надежнее схемы S и получается из S удалением подсхемы A . Заметим, что схема A реализует либо тождественную функцию, либо инверсию (поскольку схема S реализует неконстантную булеву функцию).

Схема, реализующая функцию f , отличную от константы, называется *вс-схемой*, если из нее нельзя получить более надежную схему, реализующую f или $\bar{f}$, удалением подсхемы, реализующей тождественную функцию или инверсию.

ТЕОРЕМА 6 [6]. Пусть схема S , ненадежность которой равна $P(S)$, реализует функцию f и является bc -схемой. Если в схеме S можно выделить подсхему, имеющую один вход и реализующую инверсию или тождественную функцию с вероятностями ошибок p_0 и p_1 такими, что $0 < p_0 + p_1 < 1$, то верно неравенство

$$\min\left\{\frac{p_0}{p_0 + p_1}, \frac{p_1}{p_0 + p_1}\right\} \leq P(S).$$

3. Верхние оценки ненадежности схем. Предполагается (если нет дополнительных ограничений, например, $B \subseteq B_3$), что B – произвольный полный конечный базис; а $N(S)$ – число элементов в схеме S . Докажем утверждения о верхних оценках ненадежности схем.

ЛЕММА 3. Пусть $B \cap M_1 \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_2 \cup G_3$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi(x_1, x_2, x_3) \in B \cap M_1$. Рассмотрим возможные варианты для функций $\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3}$, где $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$.

1. Случай $\sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 x_2 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_1, x_2), x_3, x_3)$. Эта схема реализует функцию из множества G_2 :

$$\begin{aligned} \varphi(\varphi(x_1, x_1, x_2), x_3, x_3) &= \varphi((\bar{x}_1 \bar{x}_1 \vee x_1 x_1 x_2), x_3, x_3) = \varphi((\bar{x}_1 \vee x_2), x_3, x_3) \\ &= \varphi((x_1 x_2 \oplus x_1 \oplus 1), x_3, x_3) = (x_1 \bar{x}_2 \oplus 1) \oplus x_3 \oplus 1 = x_1 \bar{x}_2 \oplus x_3. \end{aligned}$$

2. Случай $\sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 x_2 \vee \bar{x}_1 \bar{x}_2 x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_3, x_1), x_1, x_2)$. Эта схема реализует функцию из множества G_3 :

$$\varphi(\varphi(x_1, x_3, x_1), x_1, x_2) = \varphi(x_1 x_3, x_1, x_2) = (x_1 x_3 \vee \bar{x}_1 \bar{x}_3 \bar{x}_1 x_2) = x_1 x_3 \vee \bar{x}_1 x_2.$$

3. Случай $\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 \bar{x}_2 \vee \bar{x}_1 x_2 \bar{x}_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(x_3, \varphi(x_1, x_2, x_2), x_3)$. Эта схема реализует функцию из множества G_2 :

$$\varphi(x_3, \varphi(x_1, x_2, x_2), x_3) = \varphi(x_3, x_1 \bar{x}_2, x_3) = x_3 \bar{x}_1 \bar{x}_2 \vee \bar{x}_3 x_1 \bar{x}_2 = x_1 \bar{x}_2 \oplus x_3.$$

4. Случай $\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 \bar{x}_2 \vee \bar{x}_1 x_2 x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_2, x_1), x_3, x_3)$. Эта схема реализует функцию из множества G_2 :

$$\varphi(\varphi(x_1, x_2, x_1), x_3, x_3) = \varphi(x_1\bar{x}_2, x_3, x_3) = (x_1\bar{x}_2)\bar{x}_3 \vee \overline{(x_1\bar{x}_2)}x_3 = x_1\bar{x}_2 \oplus x_3.$$

5. Случай $\sigma_1 = 0, \sigma_2 = 1, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1x_2 \vee x_1\bar{x}_2\bar{x}_3$$

и конгруэнтна функции $x_1\bar{x}_2 \vee \bar{x}_1x_2\bar{x}_3$, рассмотренной в п. 3.

6. Случай $\sigma_1 = 0, \sigma_2 = 1, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1x_2 \vee x_1\bar{x}_2x_3$$

и конгруэнтна функции

$$x_1\bar{x}_2 \vee \bar{x}_1x_2x_3,$$

рассмотренной в п. 4.

7. Случай $\sigma_1 = 0, \sigma_2 = 0, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1\bar{x}_2 \vee x_1x_2\bar{x}_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_3, x_1), x_2, x_1)$. Эта схема реализует функцию из множества G_2 :

$$\varphi(\varphi(x_1, x_3, x_1), x_2, x_1) = \varphi(\bar{x}_1\bar{x}_3, x_2, x_1) = \overline{\bar{x}_1\bar{x}_3}\bar{x}_2 \vee \bar{x}_1\bar{x}_3x_2\bar{x}_1 = \bar{x}_1\bar{x}_3 \oplus \bar{x}_2.$$

8. Случай $\sigma_1 = 0, \sigma_2 = 0, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1\bar{x}_2 \vee x_1x_2x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_1, x_2), x_3, x_3)$. Эта схема реализует функцию из множества G_2 :

$$\varphi(\varphi(x_1, x_1, x_2), x_3, x_3) = \varphi(\overline{x_1\bar{x}_2}, x_3, x_3) = x_1\bar{x}_2\bar{x}_3 \vee \overline{x_1\bar{x}_2}x_3 = x_1\bar{x}_2 \oplus x_3.$$

Лемма 3 доказана.

ЛЕММА 4. Пусть $B \cap M_1^* \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_2 \cup G_3$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Утверждение леммы следует из теоремы 4 и леммы 3.

Обозначим

$$M'_2 = M_2 \setminus \{x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_3\},$$

а M_2^* – множество, содержащее функции, двойственные функциям множества M'_2 .

ЛЕММА 5. Пусть $B \cap M'_2 \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_2$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi(x_1, x_2, x_3) \in B \cap M'_2$. Рассмотрим возможные варианты для функции

$$\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\sigma_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} \vee x_1^{\bar{\sigma}_1} x_2^{\sigma_2} x_3^{\bar{\sigma}_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}.$$

1. Случай $\sigma_1 = 0, \sigma_2 = 0, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_1, x_3), x_1, x_2)$. Схема S_g реализует функцию из множества G_2 :

$$\varphi(\varphi(x_1, x_1, x_3), x_1, x_2) = (x_1 x_3 \oplus x_1 \oplus x_3 \oplus 1)(x_1 x_2 \oplus x_1 \oplus 1) \oplus x_1 \oplus x_2 \oplus 1 = \bar{x}_1 x_3 \oplus x_2.$$

2. Случай $\sigma_1 = 0, \sigma_2 = 0, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 \bar{x}_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 \bar{x}_3 = x_1 x_2 x_3 \oplus x_1 \oplus x_2 \oplus x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_1, x_3), x_1, x_2)$. Схема S_g реализует функцию из множества G_2 :

$$\varphi(\varphi(x_1, x_1, x_3), x_1, x_2) = (x_1 x_3 \oplus x_3)(x_1 x_2 \oplus 1) \oplus x_1 \oplus x_2 = \bar{x}_1 \bar{x}_3 \oplus \bar{x}_2.$$

3. Случай $\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 \bar{x}_2 x_3 \vee x_1 x_2 x_3 = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_1 \oplus x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(x_1, \varphi(x_1, x_3, x_1), x_2)$. Схема S_g реализует функцию из множества G_2 :

$$\varphi(x_1, \varphi(x_1, x_3, x_1), x_2) = \varphi(x_1, x_1 x_3, x_2) = (x_1 x_3)(x_1 x_2 \oplus x_1 \oplus x_2) \oplus x_1 \oplus x_2 = x_1 \bar{x}_3 \oplus x_2.$$

4. Случай $\sigma_1 = 0, \sigma_2 = 1, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 \bar{x}_2 x_3 \vee x_1 x_2 x_3 = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_2 \oplus x_3 \oplus 1.$$

Получили функцию, конгруэнтную уже рассмотренной в п. 3.

5. Случай $\sigma_1 = 0, \sigma_2 = 1, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 \bar{x}_3.$$

Получили функцию, конгруэнтную уже рассмотренной в п. 1.

6. Случай $\sigma_1 = 1, \sigma_2 = 0, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3.$$

Получили функцию, конгруэнтную уже рассмотренной в п. 1.

7. Случай $\sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 0$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 x_3 = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3 \notin M'_2.$$

8. Случай $\sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 1$. Тогда

$$\varphi(x_1, x_2, x_3) = x_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 \bar{x}_3.$$

Получили функцию, конгруэнтную уже рассмотренной в п. 3.

Лемма 5 доказана.

ЛЕММА 6. Пусть $B \cap M_2^* \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_2$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Утверждение леммы следует из теоремы 4 и леммы 5.

ЛЕММА 7. Пусть

$$\varphi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \in B.$$

Тогда в базисе B любую булеву функцию f можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 79\varepsilon^2$$

при $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Пусть f – произвольная булева функция. Искомую схему S , реализующую функцию f , будем строить в три этапа.

Этап 1. Сначала построим схему S_g , которая реализует функцию голосования

$$g = x_1x_2 \vee x_1x_3 \vee x_2x_3 \in G_1$$

и будет использована для повышения надежности исходных схем.

По теореме 1 для функций f_1, f_2, f_3 , где

$$f_1(x_1, x_2, x_3) = x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$$

и

$$f_2(x_1, x_2, x_3) = f_3(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3,$$

можно построить соответственно схемы F_1, F_2, F_3 , функционирующие с ненадежностью $P(F_1) \leq 5.2\varepsilon$, $P(F_2) = P(F_3) \leq 5.2\varepsilon$. Используя схемы F_1, F_2 и F_3 и два элемента, реализующих функцию φ , построим схему S_g (рис. 4). Проверим, что схема S_g реализует функцию голосования $g = x_1x_2 \vee x_1x_3 \vee x_2x_3$. Действительно,

$$\varphi(f_1, f_2, f_3) = x_1x_2 \oplus x_1x_3, \quad \varphi(\varphi(f_1, f_2, f_3), x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 = g.$$

Ненадежность схемы S_g удовлетворяет неравенству

$$P(S_g) \leq P(F_1) + P(F_2) + P(F_3) + 2\varepsilon \leq 17.6\varepsilon.$$

Оценим вероятности ошибок v^0 и v^1 схемы S_g на характеристических наборах $(1, 1, 1)$ и $(0, 0, 0)$ соответственно. Нетрудно видеть, что ошибка в точности одной из схем F_1, F_2 или F_3 на входных наборах $(0, 0, 0)$ и $(1, 1, 1)$ не приводит к появлению ошибки на выходе всей схемы S_g . Чтобы ошибка на выходе схемы S_g произошла, нужно чтобы ошиблась подсхема $S_{2\varphi}$ или чтобы ошиблись хотя бы две из схем F_1, F_2, F_3 . Таким образом, вероятность ошибки v^0 схемы S_g на наборе $(1, 1, 1)$ удовлетворяет неравенству:

$$v^0 \leq P(S_{2\varphi}) + \sum_{i=2}^3 C_3^i (5.2\varepsilon)^i \leq 2\varepsilon + 3(5.2\varepsilon)^2 + (5.2\varepsilon)^3 \leq 2\varepsilon + 81.3\varepsilon^2.$$

Рис. 4. Схема S_g

Аналогично получается верхняя оценка для вероятности ошибки v^1 схемы S_g на наборе $(0, 0, 0)$. Поэтому $v^1 \leq 2\varepsilon + 81.3\varepsilon^2$.

Пусть f – произвольная булева функция. Возьмем три экземпляра схемы S_f , каждая из которых реализует функцию f . Соединим выход i -й схемы S_f с i -м, $i = 1, 2, 3$, входом схемы S_g , реализующей функцию голосования

$$g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Нетрудно видеть, что построенная таким образом схема (обозначим ее $\chi(S_f)$) реализует функцию f . По теореме 2 имеем

$$P(\chi(S_f)) \leq 2\varepsilon + 81.3\varepsilon^2 + 3 \cdot 5.2\varepsilon \cdot 17.6\varepsilon + 3 \cdot (5.2\varepsilon)^2 \leq 2\varepsilon + 434\varepsilon^2 \leq 2.46\varepsilon$$

при $\varepsilon \in (0, 1/960]$.

Прделаем еще один шаг итерации. По схеме $\chi(S_f)$ построим схему $\chi^2(S_f)$ следующим образом: возьмем три экземпляра схемы $\chi(S_f)$, каждая из которых реализует функцию f и один экземпляр схемы S_g . Соединим выход i -й схемы $\chi(S_f)$ с i -м входом схемы S_g , $i = 1, 2, 3$. Построенная схема $\chi^2(S_f)$ реализует функцию f . По теореме 2 оценим ее ненадежность и получим

$$P(\chi^2(S_f)) \leq 2\varepsilon + 81.3\varepsilon^2 + 3 \cdot 2.46\varepsilon \cdot 17.6\varepsilon + 3 \cdot (2.46\varepsilon)^2 \leq 2\varepsilon + 230\varepsilon^2 \leq 2.24\varepsilon.$$

Таким образом, для любой булевой функции f можно построить такую схему S , что

$$P(S) \leq 2.24\varepsilon \quad \text{при} \quad \varepsilon \in (0, 1/960].$$

Этап 2. Снова возьмем схему S_g на рис. 4, но теперь считаем, что каждая из схем F_1 , F_2 и F_3 функционирует с ненадежностью $P(F_i) \leq 2.24\varepsilon$, $i = 1, 2, 3$. Тогда для ненадежности $P(S_g)$ схемы S_g верно неравенство

$$P(S_g) \leq P(F_1) + P(F_2) + P(F_3) + 2\varepsilon \leq 8.72\varepsilon.$$

Оценим вероятность ошибки v^0 схемы S_g на наборе $(1, 1, 1)$ аналогично тому, как это сделано на первом этапе:

$$v^0 \leq P(S_{2\varphi}) + \sum_{i=2}^3 C_3^i (2.24\varepsilon)^i \leq 2\varepsilon + 3(2.24\varepsilon)^2 + (2.24\varepsilon)^3 \leq 2\varepsilon + 15.1\varepsilon^2.$$

Аналогично получается верхняя оценка для вероятности ошибки v^1 схемы S_g на наборе $(0, 0, 0)$. Поэтому

$$v^1 \leq 2\varepsilon + 3(2.24\varepsilon)^2 + (2.24\varepsilon)^3 \leq 2\varepsilon + 15.1\varepsilon^2.$$

Пусть f – произвольная булева функция. Возьмем три экземпляра схемы S_f , каждая из которых реализует функцию f с ненадежностью не больше 2.24ε . Соединим выход i -й схемы S_f с i -м, $i = 1, 2, 3$, входом схемы S_g , реализующей функцию голосования

$$g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Нетрудно видеть, что построенная таким образом схема реализует функцию f . Обозначим эту схему $\chi(S_f)$. По теореме 2 имеем

$$P(\chi(S_f)) \leq 2\varepsilon + 15.1\varepsilon^2 + 3 \cdot 2.24\varepsilon \cdot 8.72\varepsilon + 3 \cdot (2.24\varepsilon)^2 \leq 2\varepsilon + 89\varepsilon^2 \leq 2.1\varepsilon$$

при $\varepsilon \in (0, 1/960]$.

Этап 3. Снова возьмем схему S_g на рис. 4, но теперь считаем, что каждая из схем F_1 , F_2 и F_3 функционирует с ненадежностью $P(F_i) \leq 2.1\varepsilon$, $i = 1, 2, 3$. Тогда для ненадежности $P(S_g)$ схемы S_g верно неравенство

$$P(S_g) \leq P(F_1) + P(F_2) + P(F_3) + 2\varepsilon \leq 8.3\varepsilon.$$

Оценим вероятность ошибки v^0 схемы S_g на наборе $(1, 1, 1)$ аналогично тому, как это сделано на первом этапе, и получим неравенство

$$v^0 \leq P(S_{2\varphi}) + \sum_{i=2}^3 C_3^i (2.1\varepsilon)^i \leq 2\varepsilon + 13.3\varepsilon^2.$$

Аналогично получается верхняя оценка для вероятности ошибки v^1 схемы S_g на наборе $(0, 0, 0)$. Поэтому

$$v^1 \leq 2\varepsilon + 13.3\varepsilon^2.$$

Пусть f – произвольная булева функция. Возьмем три экземпляра схемы S_f , каждая из которых реализует функцию f с ненадежностью не больше 2.1ε . Соединим выход i -й схемы S_f с i -м, $i = 1, 2, 3$, входом схемы S_g , реализующей функцию голосования

$$g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Нетрудно видеть, что построенная таким образом схема (обозначим ее $\chi(S_f)$) реализует функцию f . По теореме 2 имеем

$$P(\chi(S_f)) \leq 2\varepsilon + 13.3\varepsilon^2 + 3 \cdot 2.1\varepsilon \cdot 8.3\varepsilon + 3 \cdot (2.1\varepsilon)^2 \leq 2\varepsilon + 79\varepsilon^2.$$

Схема $\chi(S_f) = S$ искомая. Лемма 7 доказана.

ЗАМЕЧАНИЕ 1. При доказательстве леммы 7 можно было бы проделать еще несколько этапов. На этапе 4, учитывая, что $2\varepsilon + 79\varepsilon^2 \leq 2.0823\varepsilon$ при $\varepsilon \in (0, 1/960]$, получим

- $P(S_g) \leq 8.247\varepsilon$ вместо $P(S_g) \leq 8.3\varepsilon$;
- $v^0, v^1 \leq 2\varepsilon + 13.02\varepsilon^2$ вместо $v^0, v^1 \leq 2\varepsilon + 13.3\varepsilon^2$;
- $P(\chi(S_f)) \leq 2\varepsilon + 77.57\varepsilon^2$ вместо $P(\chi(S_f)) \leq 2\varepsilon + 79\varepsilon^2$.

На этапе 5, учитывая, что $2\varepsilon + 77.57\varepsilon^2 \leq 2.081\varepsilon$ при $\varepsilon \in (0, 1/960]$, получим

- $P(S_g) \leq 8.243\varepsilon$ вместо $P(S_g) \leq 8.247\varepsilon$;
- $v^0, v^1 \leq 2\varepsilon + 13.0011\varepsilon^2$ вместо $v^0, v^1 \leq 2\varepsilon + 13.02\varepsilon^2$;
- $P(\chi(S_f)) \leq 2\varepsilon + 77.46\varepsilon^2$ вместо $P(\chi(S_f)) \leq 2\varepsilon + 77.57\varepsilon^2$.

Из этих неравенств видно, что на этапах 4 и 5 вероятности ошибок уменьшились незначительно, на следующих этапах существенных изменений в оценках вероятностей ошибок не будет. Поэтому авторы приняли решение ограничиться тремя этапами. Формулировки и доказательства теорем 8 и 10 также являются результатом аналогичных рассуждений.

ЛЕММА 8. Пусть $\varphi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_3$ и $\varphi^* \in B$. Тогда в базисе B любую булеву функцию f можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 79\varepsilon^2$$

при $\varepsilon \in (0, 1/960]$.

Утверждение леммы следует из теоремы 4 и леммы 7.

ЛЕММА 9. Пусть $B \cap M_3 \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g \in G_4$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi(x_1, x_2, x_3) \in B \cap M_3$. Рассмотрим возможные варианты для функции $\varphi = \bar{x}_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$, где $\sigma_2, \sigma_3 \in \{0, 1\}$. Возможны 3 случая:

- 1) если $\sigma_2 = \sigma_3$, то из $\varphi(x_1, x_2, x_3)$ подстановкой z_1 вместо x_1 и подстановкой z_2 вместо x_2 и x_3 возможно получить функцию $\phi_1(z_1, z_2) = \bar{z}_1z_2^{\sigma_2}$;
- 2) если $\sigma_2 = 0, \sigma_3 = 1$, то из $\varphi(x_1, x_2, x_3)$ подстановкой z_1 вместо x_1 и x_3 , z_2 вместо x_2 возможно получить функцию $\phi_2(z_1, z_2) = \bar{z}_1\bar{z}_2$;
- 3) если $\sigma_2 = 1, \sigma_3 = 0$, то из $\varphi(x_1, x_2, x_3)$ подстановкой z_1 вместо x_1 и x_2 , z_2 вместо x_3 возможно получить функцию $\phi_2(z_1, z_2) = \bar{z}_1\bar{z}_2$.

Тогда функция

$$\begin{aligned} \varphi(\phi_i(z_1, z_2), x_2, x_3) &= \bar{z}_1z_2^a(x_2^{\sigma_2} \vee x_3^{\sigma_3}) = (z_1 \vee \bar{z}_2^a)(x_2^{\sigma_2} \vee x_3^{\sigma_3}) \\ &= g(z_1, z_2, x_2, x_3) \in G_4, \quad i \in \{1, 2\}, \quad a \in \{0, 1\}. \end{aligned}$$

Очевидно, что функцию $\phi(z_1, z_2, x_2, x_3)$ можно реализовать схемой S_g из двух элементов.

Лемма 9 доказана.

ЛЕММА 10. Пусть $B \cap M_3^* \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_4$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Утверждение леммы следует из теоремы 4 и леммы 9.

ЛЕММА 11. Пусть $B \cap M_4 \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_1$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi(x_1, x_2, x_3) \in B \cap M_4$. Рассмотрим возможные варианты для функции

$$\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3}, \quad \text{где } \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}.$$

1. Пусть

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3 = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(\varphi(x_1, x_2, x_3), x_1, x_1)$. Схема S_g реализует функцию из множества G_1 :

$$\varphi(\varphi(x_1, x_2, x_3), x_1, x_1) = \bar{x}_1 x_2 \oplus \bar{x}_1 x_3 \oplus x_2 x_3.$$

2. Пусть

$$\varphi(x_1, x_2, x_3) = \bar{x}_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_3.$$

Построим схему S_g из двух элементов, моделируя формулу $\varphi(x_1, x_1, \varphi(x_1, x_2, x_3))$. Схема S_g реализует функцию из множества G_1 :

$$\varphi(x_1, x_1, \varphi(x_1, x_2, x_3)) = x_1 \bar{x}_2 \oplus x_1 x_3 \oplus \bar{x}_2 x_3.$$

Лемма 11 доказана.

ЛЕММА 12. Пусть $B \cap M_4^* \neq \emptyset$. Тогда в базисе B можно построить такую схему S_g , реализующую функцию $g(x_1, x_2, x_3) \in G_1$, что $N(S_g) = 2$.

ДОКАЗАТЕЛЬСТВО. Утверждение леммы следует из теоремы 4 и леммы 11.

ЗАМЕЧАНИЕ 2. Леммы 3–12 справедливы, если в полном конечном базисе B содержится функция, из которой подстановкой переменных можно получить некоторую функцию множества M .

ЛЕММА 13. Пусть схема S_ϕ реализует функцию $\phi \in G_2$, т.е. функцию вида

$$x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\},$$

с ненадежностью $P(S_\phi) = p_\phi$. Тогда можно построить такую схему S_g , реализующую функцию

$$g = x_1^{\sigma_3} \bar{x}_2 \vee x_1^{\sigma_3} \bar{x}_3 \vee \bar{x}_2 \bar{x}_3 \in G_1,$$

что $P(S_g) \leq p_\phi + 2p_\oplus$ ($p_\oplus$ – максимальная из ненадежностей схем, реализующих функции $x_1 \oplus x_2$ и $x_1 \oplus x_2 \oplus 1$), а для вероятностей ошибок v^1 и v^0 схемы S_g на наборах $(\bar{\sigma}_3, 1, 1)$ и $(\sigma_3, 0, 0)$ соответственно выполняются неравенства

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2.$$

ДОКАЗАТЕЛЬСТВО. Пусть функция

$$\phi = x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3} \in G_2, \quad \text{где } \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}.$$

Реализуем функции $(x_1 \oplus x_2)^{\sigma_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\sigma_2 \oplus \sigma_3}$ схемами $S_{\oplus \sigma_1}$ и $S_{\oplus \sigma_2}$ соответственно и будем считать, что $p_{\oplus} = \max\{P(S_{\oplus \sigma_1}), P(S_{\oplus \sigma_2})\}$. Построим схему S_g (см. рис. 5), которая реализует функцию

$$\begin{aligned} \phi((x_1 \oplus x_2)^{\sigma_1 \oplus \sigma_3}, (x_1 \oplus x_3)^{\sigma_2 \oplus \sigma_3}, x_1) &= (x_1 \oplus x_2 \oplus \sigma_3)(x_1 \oplus x_3 \oplus \sigma_3) \oplus x_1^{\sigma_3} \\ &= x_1^{\bar{\sigma}_3} x_2 \oplus x_1^{\bar{\sigma}_3} x_3 \oplus x_2 x_3 \oplus 1 \\ &= x_1^{\sigma_3} \bar{x}_2 \vee x_1^{\sigma_3} \bar{x}_3 \vee \bar{x}_2 \bar{x}_3 \in G_1. \end{aligned}$$

Схема S_g имеет ненадежность $P(S_g) \leq p_{\phi} + 2p_{\oplus}$.

Рис. 5. Схема S_g

Для схемы S_g (см. рис. 5) вычислим и оценим вероятности ошибок v^0, v^1 на наборах $\tilde{\alpha} = (\sigma_3, 0, 0)$ и $\tilde{\beta} = (\bar{\sigma}_3, 1, 1)$ соответственно: $v^0, v^1 \leq p_{\phi} + 2p_{\phi} p_{\oplus} + p_{\oplus}^2$.

Лемма 13 доказана.

ЛЕММА 14. Пусть схема S_{ϕ} реализует функцию $\phi \in G_3$, т.е. функцию вида

$$x_1^{\sigma_1} x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\},$$

с ненадежностью $P(S_{\phi}) = p_{\phi}$. Тогда можно построить такую схему S_g , реализующую функцию

$$g = x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2^{\sigma_2} x_3^{\sigma_3} \in G_1,$$

что $P(S_g) \leq 2p_{\phi}$, а для вероятностей ошибок v^1 и v^0 схемы S_g на наборах $(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3)$ и $(\sigma_1, \sigma_2, \sigma_3)$ соответственно выполняются неравенства $v^1, v^0 \leq p_{\phi}$.

ДОКАЗАТЕЛЬСТВО. Пусть $\phi \in G_3$. Без ограничения общности можно считать, что $\phi = x_1^{\sigma_1} \bar{x}_2 \vee x_2 x_3^{\sigma_3}$. Тогда, моделируя формулу $\phi(x_1, \phi(x_1, x_2, x_3), x_3)$, построим схему S_g , реализующую функцию $x_1^{\sigma_1} x_2 \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2 x_3^{\sigma_3}$. Имеем $P(S_g) \leq 2p_{\phi}$.

Оценим вероятности ошибок v^1 и v^0 схемы S_g на наборах $\tilde{\alpha} = (\bar{\sigma}_1, 0, \bar{\sigma}_3)$ и $\tilde{\beta} = (\sigma_1, 1, \sigma_3)$ соответственно и получим $v^1, v^0 \leq p_{\phi}$.

Лемма 14 доказана.

ТЕОРЕМА 7. Пусть B – базис такой, что $B \cap M \neq \emptyset$. Тогда любую булеву функцию f в базисе B можно реализовать такой схемой C , что $P(C) \leq 2\varepsilon + 79\varepsilon^2$ для всех $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Пусть f – произвольная булева функция. По теореме 1 функцию f в базисе B можно реализовать схемой с ненадежностью $p \leq 5.2\varepsilon$.

Пусть $\varphi \in M \cap B$. Возможны следующие случаи.

Случай 1. Если функция $\varphi \in (M_1 \cup M'_2 \cup M_1^* \cup M_2^{*'}) \cap B$, то по леммам 3–6 некоторую функцию $\phi \in G_2 \cup G_3$ можно реализовать схемой S_ϕ из двух элементов. Поэтому $P(S_\phi) = p_\phi \leq 2\varepsilon$. Рассмотрим два случая: $\phi \in G_2$ и $\phi \in G_3$.

1.1. Пусть $\phi \in G_2$ и $\phi = x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3}$, $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$. Требуемую схему для функции f построим в 2 этапа.

Этап 1. Используя теорему 1, реализуем функции $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ схемами с ненадежностью $p_\oplus \leq 5.2\varepsilon$. Используя эти схемы и применяя лемму 13, строим схему S_g^1 ($g \in G_1$), для которой

$$P(S_g^1) \leq p_\phi + 2p_\oplus \leq 2\varepsilon + 2 \cdot 5.2\varepsilon = 12.4\varepsilon,$$

а вероятности ошибок v^1 и v^0 на характеристических наборах удовлетворяют неравенствам

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2 \leq 2\varepsilon + 2 \cdot 2\varepsilon \cdot 5.2\varepsilon + (5.2\varepsilon)^2 \leq 2\varepsilon + 48\varepsilon^2.$$

Воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_1 , что

$$\begin{aligned} P(S_1) &\leq \max\{v^0, v^1\} + 3pP(S_g^1) + 3p^2 \\ &\leq 2\varepsilon + 48\varepsilon^2 + 3 \cdot 5.2\varepsilon \cdot 12.4\varepsilon + 3(5.2\varepsilon)^2 \leq 2\varepsilon + 323\varepsilon^2 \leq 2.34\varepsilon \end{aligned}$$

при $\varepsilon \in (0, 1/960]$.

Этап 2. Поскольку произвольную функцию f можно реализовать схемой с ненадежностью $p \leq 2.34\varepsilon$, для функций $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ построим схемы с ненадежностью $p_\oplus \leq 2.34\varepsilon$. Затем, применяя лемму 13, построим такую схему S_g^2 , что

$$P(S_g^2) \leq p_\phi + 2p_\oplus \leq 2\varepsilon + 2 \cdot 2.34\varepsilon = 6.68\varepsilon,$$

а вероятности ошибок v^1 и v^0 удовлетворяют неравенствам

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2 \leq 2\varepsilon + 2 \cdot 2\varepsilon \cdot 2.34\varepsilon + (2.34\varepsilon)^2 \leq 2\varepsilon + 15\varepsilon^2.$$

Далее воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_2 , что

$$P(S_2) \leq \max\{v^0, v^1\} + 3pP(S_g^2) + 3p^2 \leq 2\varepsilon + 15\varepsilon^2 + 3 \cdot 2.34\varepsilon \cdot 6.68\varepsilon + 3(2.34\varepsilon)^2 \leq 2\varepsilon + 79\varepsilon^2.$$

Схема $S_2 = C$ искомая.

1.2. Пусть $\phi \in G_3$ и $\phi = x_1^{\sigma_1} x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2} x_3^{\sigma_3}$, $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$. Тогда по лемме 14 схеме S_g^3 , $g \in G_1$, можно построить с ненадежностью $P(S_g^3) \leq 2p_\phi \leq 4\varepsilon$ и вероятностями ошибок на характеристических наборах: $v^1, v^0 \leq P(S_\phi) = p_\phi \leq 2\varepsilon$.

Воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_3 , что

$$P(S_3) \leq \max\{v^0, v^1\} + 3pP(S_g^3) + 3p^2 \leq 2\varepsilon + 3 \cdot 4\varepsilon \cdot 5.2\varepsilon + 3(5.2\varepsilon)^2 \leq 2\varepsilon + 144\varepsilon^2 \leq 2.15\varepsilon$$

при $\varepsilon \in (0, 1/960]$.

Теперь полагаем, что $p \leq 2.15\varepsilon$, и снова воспользуемся теоремой 2, по которой любую функцию f можно реализовать такой схемой S_4 , что

$$P(S_4) \leq \max\{v^0, v^1\} + 3pP(S_g^3) + 3p^2 \leq 2\varepsilon + 3 \cdot 4\varepsilon \cdot 2.15\varepsilon + 3(2.15\varepsilon)^2 \leq 2\varepsilon + 40\varepsilon^2.$$

Схема $S_4 = C$ искомая.

Случай 2. Если функция

$$\varphi = x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_3$$

и $\{\varphi, \varphi^*\} \cap B \neq \emptyset$, то по леммам 7, 8 можно любую функцию реализовать схемой S_5 , ненадежность которой $P(S_5) \leq 2\varepsilon + 79\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Схема $S_5 = C$ искомая.

Случай 3. Если функция $\varphi \in (M_3 \cup M_3^*) \cap B$, то по леммам 9, 10 можно построить схему S_g^5 из двух элементов (т.е. $N(S_g^5) = 2$), реализующую функцию $g \in G_4$.

Воспользуемся леммой 1, по которой функцию f можно реализовать такой схемой S_6 , что

$$P(S_6) \leq N(S_g^5)\varepsilon + 6p^2 \leq 2\varepsilon + 6(5.2\varepsilon)^2 \leq 2\varepsilon + 162.3\varepsilon^2 \leq 2.17\varepsilon$$

при $\varepsilon \in (0, 1/960]$.

Повторно воспользуемся леммой 1 (учитывая, что $p \leq 2.17\varepsilon$), по которой функцию f можно реализовать такой схемой S_7 , что

$$P(S_7) \leq N(S_g^5)\varepsilon + 6p^2 \leq 2\varepsilon + 6(2.17\varepsilon)^2 \leq 2\varepsilon + 29\varepsilon^2.$$

Схема $S_7 = C$ искомая.

Случай 4. Если функция $\varphi \in (M_4 \cup M_4^*) \cap B$, то по леммам 11, 12 можно построить схему S_g^6 из двух элементов (т.е. $N(S_g^6) = 2$), реализующую функцию $g \in G_1$.

Воспользуемся леммой 1, по которой функцию f можно реализовать такой схемой S_8 , что

$$P(S_8) \leq N(S_g^6)\varepsilon + 6p^2 \leq 2\varepsilon + 6(5.2\varepsilon)^2 \leq 2\varepsilon + 162.3\varepsilon^2 \leq 2.17\varepsilon$$

при $\varepsilon \in (0, 1/960]$. Повторно воспользуемся леммой 1 (учитывая, что $p \leq 2.17\varepsilon$), по которой функцию f можно реализовать такой схемой S_9 , что

$$P(S_9) \leq N(S_g^6)\varepsilon + 6p^2 \leq 2\varepsilon + 6(2.17\varepsilon)^2 \leq 2\varepsilon + 29\varepsilon^2.$$

Схема $S_9 = C$ искомая.

Теорема 7 доказана.

ЛЕММА 15. Пусть $\varphi \in \Psi$. Тогда отождествлением переменных из φ можно получить функцию вида $x_1^a x_2^b$, $a, b \in \{0, 1\}$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi = x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3}$ и $\sigma_i = \sigma_j$, тогда после отождествления i -й и j -й переменных получим функцию вида

$$x_k^{\sigma_k} x_i^{\sigma_i}, \quad i, j, k \in \{1, 2, 3\}, \quad i, j, k \text{ попарно различны}, \quad \sigma_i, \sigma_j, \sigma_k \in \{0, 1\}.$$

Пусть $\varphi = x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$. Если $\sigma_2 = \sigma_3$, тогда после отождествления 2-й и 3-й переменных получим функцию вида $x_1 x_2^{\sigma_2}$. Если $\sigma_2 \neq \sigma_3$, то найдется такое $i \in \{2, 3\}$, что $\sigma_i = 0$. Тогда отождествлением 1-й и i -й переменных получим функцию

$$x_1 x_j^{\sigma_j}, \quad j \in \{2, 3\} \setminus \{i\}.$$

Пусть $\varphi = x_1^{\sigma_1}(x_2^{\sigma_2} x_3^{\sigma_3} \vee x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3})$. Если $\sigma_2 = \sigma_3$, то после отождествления 1-й со 2-й или 1-й с 3-й переменных получим функцию вида $x_1^{\sigma_1} x_k^{\tau_k}$, $\tau_k \in \{0, 1\}$, $k \in \{2, 3\}$. Если $\sigma_2 \neq \sigma_3$, то найдется такое $i \in \{2, 3\}$, что $\sigma_i \neq \sigma_1$. Тогда отождествлением первой и i -й переменных получим функцию

$$x_1^{\sigma_1} x_j^{\sigma_j}, \quad j \in \{2, 3\} \setminus \{i\}.$$

Лемма 15 доказана.

ЛЕММА 16. Пусть $\varphi \in \Psi^*$. Тогда отождествлением переменных из φ можно получить функцию вида

$$x_1^a \vee x_2^b, \quad a, b \in \{0, 1\}.$$

ДОКАЗАТЕЛЬСТВО. Утверждение леммы следует из теоремы 4 и леммы 15.

ТЕОРЕМА 8. Пусть B – полный базис, $B \subseteq (\tilde{\Psi} \cup M_5)$, $B \cap M_5 \neq \emptyset$. Тогда любую функцию f можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 65\varepsilon^2$$

при $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Поскольку $B \subseteq (\tilde{\Psi} \cup M_5)$ и $B \cap M_5 \neq \emptyset$, некоторую функцию вида

$$\phi(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3} \in G_2, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\},$$

можно реализовать схемой A , используя ровно 2 элемента и действуя следующим образом: по леммам 15 и 16 из функций множества $\tilde{\Psi}$ можно получить некоторую функцию вида $(x_1^{c_1} x_2^{c_2})^b$, используя один функциональный элемент.

Если базис содержит функцию $\eta = x_1 \oplus x_2 \oplus a$, $a \in \{0, 1\}$, то, моделируя формулу $\eta((x_1^{c_1} x_2^{c_2})^b, x_3)$, $b, c_1, c_2 \in \{0, 1\}$, строим схему A из двух элементов, реализующую функцию

$$x_1^{c_1} x_2^{c_2} \oplus \bar{b} \oplus x_3 \oplus a = x_1^{c_1} x_2^{c_2} \oplus x_3^{a \oplus b} = \phi(x_1, x_2, x_3).$$

Если базис содержит функцию $\eta = x_1 \oplus x_2 \oplus x_3 \oplus a$, $a \in \{0, 1\}$, то, моделируя формулу $\eta((x_1^{c_1} x_2^{c_2})^b, x_2, x_3)$, $b, c_1, c_2 \in \{0, 1\}$, строим схему A из двух элементов, реализующую функцию

$$x_1^{c_1} x_2^{c_2} \oplus \bar{b} \oplus x_2 \oplus x_3 \oplus a = x_1^{c_1} x_2^{c_2} \oplus x_3^{a \oplus b \oplus \bar{c}_2} = \phi(x_1, x_2, x_3).$$

Таким образом, и в первом, и во втором случаях построена схема A из двух элементов. Следовательно, $P(A) = p_\phi \leq 2\varepsilon$.

По теореме 1 любую булеву функцию можно реализовать такой схемой, ненадежность которой $p \leq 5.2\varepsilon$ при $\varepsilon \in (0; 1/960]$. Требуемую схему S будем строить в три этапа.

Этап 1. Используя теорему 1, реализуем функции $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_2 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ схемами с ненадежностью $p_\oplus \leq 5.2\varepsilon$. Применяя лемму 13, строим схему S_g^1 , $g \in G_1$, для которой

$$P(S_g^1) \leq p_\phi + 2p_\oplus \leq 2\varepsilon + 2 \cdot 5.2\varepsilon = 12.4\varepsilon,$$

а вероятности ошибок v^1 и v^0 на характеристических наборах удовлетворяют неравенствам

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2 \leq 2\varepsilon + 2 \cdot 2\varepsilon \cdot 5.2\varepsilon + (5.2\varepsilon)^2 \leq 2\varepsilon + 48\varepsilon^2.$$

Воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_1 , что

$$\begin{aligned} P(S_1) &\leq \max\{v^0, v^1\} + 3pP(S_g^1) + 3p^2 \\ &\leq 2\varepsilon + 48\varepsilon^2 + 3 \cdot 5.2\varepsilon \cdot 12.4\varepsilon + 3(5.2\varepsilon)^2 \leq 2\varepsilon + 323\varepsilon^2 \leq 2.34\varepsilon \end{aligned}$$

при $\varepsilon \in (0, 1/960]$.

Этап 2. Поскольку произвольную функцию f можно реализовать схемой с ненадежностью $p \leq 2.34\varepsilon$, для функций $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ построим схемы с ненадежностью $p_\oplus \leq 2.34\varepsilon$. Затем, применяя лемму 13, построим такую схему S_g^2 , что

$$P(S_g^2) \leq p_\phi + 2p_\oplus \leq 2\varepsilon + 2 \cdot 2.34\varepsilon = 6.68\varepsilon,$$

а вероятности ошибок v^1 и v^0 удовлетворяют неравенствам

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2 \leq 2\varepsilon + 2 \cdot 2\varepsilon \cdot 2.34\varepsilon + (2.34\varepsilon)^2 \leq 2\varepsilon + 15\varepsilon^2.$$

Далее воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_2 , что

$$\begin{aligned} P(S_2) &\leq \max\{v^0, v^1\} + 3pP(S_g^2) + 3p^2 \\ &\leq 2\varepsilon + 15\varepsilon^2 + 3 \cdot 2.34\varepsilon \cdot 6.68\varepsilon + 3(2.34\varepsilon)^2 \leq 2\varepsilon + 79\varepsilon^2 \leq 2.083\varepsilon \end{aligned}$$

при $\varepsilon \in (0, 1/960]$.

Этап 3. Поскольку произвольную функцию f можно реализовать схемой с ненадежностью $p \leq 2.083\varepsilon$, для функций $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ построим схемы с ненадежностью $p_\oplus \leq 2.083\varepsilon$. Затем, применяя лемму 13, построим такую схему S_g^3 , что

$$P(S_g^3) \leq p_\phi + 2p_\oplus \leq 2\varepsilon + 2 \cdot 2.083\varepsilon = 6.166\varepsilon,$$

а вероятности ошибок v^1 и v^0 удовлетворяют неравенствам

$$v^1, v^0 \leq p_\phi + 2p_\phi p_\oplus + p_\oplus^2 \leq 2\varepsilon + 2 \cdot 2\varepsilon \cdot 2.083\varepsilon + (2.083\varepsilon)^2 \leq 2\varepsilon + 13\varepsilon^2.$$

Далее, воспользуемся теоремой 2, по которой функцию f можно реализовать такой схемой S_3 , что

$$\begin{aligned} P(S_3) &\leq \max\{v^0, v^1\} + 3pP(S_g^3) + 3p^2 \\ &\leq 2\varepsilon + 13\varepsilon^2 + 3 \cdot 2.083\varepsilon \cdot 6.166\varepsilon + 3(2.083\varepsilon)^2 \leq 2\varepsilon + 65\varepsilon^2. \end{aligned}$$

Схема $S_3 = S$ искомая. Теорема 8 доказана.

Следующая теорема является обобщением теоремы 8.

ТЕОРЕМА 9. Пусть в полном базисе B содержится линейная функция, существенно зависящая не менее чем от двух переменных. Тогда любую функцию f в базисе B можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 65\varepsilon^2$$

при всех $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Поскольку базис B полный, в нем содержится нелинейная функция $\psi(x_1, x_2, \dots, x_m)$, $m \geq 2$.

По лемме 2 подстановкой переменных из функции $\psi(x_1, x_2, \dots, x_m)$ можно получить либо функцию

$$\begin{aligned} \varphi_1(x_1, x_2, x_3) &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0, \\ a_0, a_1, a_2, a_3 &\in \{0, 1\}, \end{aligned}$$

либо

$$\varphi_2(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0, \quad a_0, a_1, a_2, a_3 \in \{0, 1\}.$$

Случай 1. Пусть подстановкой переменных из функции $\psi(x_1, x_2, \dots, x_m)$ можно получить функцию вида

$$\begin{aligned} \varphi_1(x_1, x_2, x_3) &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0, \\ a_i &\in \{0, 1\}, \quad i \in \{0, 1, 2, 3\}. \end{aligned}$$

При различных значениях коэффициентов a_0, a_1, a_2, a_3 может получиться 16 различных функций $\varphi_1(x_1, x_2, x_3)$. Рассмотрим возможные случаи.

Подслучай 1.1:

$$x_1x_2 \oplus x_1x_3 \oplus x_2x_3, \quad x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1$$

(если коэффициенты a_1, a_2, a_3 равны нулю). Обе функции принадлежат множеству G_1 .

Подслучай 1.2:

$$\begin{aligned} x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_2 \oplus a_0 &= x_1x_2 \oplus x_1\bar{x}_3 \oplus x_2\bar{x}_3 \oplus a_0, \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_3 \oplus a_0, &\quad x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus a_0, \end{aligned}$$

$a_0 \in \{0, 1\}$. В этом случае все шесть функций также принадлежат множеству G_1 .

В каждом из двух рассмотренных случаев по теореме 3 получаем, что в базисе B любую функцию f можно реализовать схемой S с ненадежностью $P(S) \leq \varepsilon + 8\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Подслучай 1.3:

$$\begin{aligned} x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus a_0, & \quad x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus a_0, \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 \oplus a_0, & \quad x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus a_0, \end{aligned}$$

$a_0 \in \{0, 1\}$. Каждая из этих восьми функций может быть представлена в виде

$$(x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3})^{\sigma_4}, \quad \sigma_i \in \{0, 1\}, \quad i \in \{1, 2, 3, 4\}.$$

Все восемь функций принадлежат множеству $M_4 \cup M_4^*$. Повторим рассуждения пункта 4 из теоремы 7 и получим, что в базисе B любую функцию f можно реализовать схемой S с ненадежностью $P(S) \leq 2\varepsilon + 29\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Случай 2. Пусть с помощью подстановки переменных из нелинейной функции $\psi(x_1, x_2, \dots, x_m)$ можно получить функцию

$$\varphi_2(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0 \quad a_0, a_1, a_2 \in \{0, 1\}.$$

Поскольку базис B содержит линейную функцию, существенно зависящую от двух или более переменных, из нее подстановкой переменных можно получить функцию множества M_5 . Тогда по теореме 8 в базисе B любую функцию f можно реализовать такой схемой S , что $P(S) \leq 2\varepsilon + 65\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Теорема 9 доказана.

ТЕОРЕМА 10. Пусть полный базис B содержит функцию $\varphi(x_1, x_2, x_3)$, конгруэнтную функции вида $x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$, $\sigma_2, \sigma_3 \in \{0, 1\}$, и $B \cap \Psi^* \neq \emptyset$. Тогда любую булеву функцию f в базисе B можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 25\varepsilon^2$$

при $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Пусть B – полный базис, $B \cap \Psi^* \neq \emptyset$ и

$$\varphi(x_1, x_2, x_3) = x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}) \in B, \quad \sigma_2, \sigma_3 \in \{0, 1\}.$$

По лемме 16 из любой функции $h \in \Psi^*$ отождествлением переменных можно получить функцию $h'(x_1, x_4) = x_1^a \vee x_4^b$, $a, b \in \{0, 1\}$. Моделируя формулу $\varphi(h'(x_1, x_4), x_2, x_3)$, построим схему S_g из двух элементов, реализующую функцию

$$g = (x_1^a \vee x_4^b)(x_2^{\sigma_2} \vee x_3^{\sigma_3}) \in G_4, \quad a, b, \sigma_1, \sigma_2 \in \{0, 1\}.$$

По теореме 1 любую булеву функцию можно реализовать такой схемой, ненадежность которой $p \leq 5.2\varepsilon$ при $\varepsilon \in (0, 1/960]$. Воспользуемся леммой 1 (учитывая, что $N(S_g) = 2$), по которой функцию f можно реализовать такой схемой S_1 , что

$$P(S_1) \leq N(S_g)\varepsilon + 6p^2 \leq 2\varepsilon + 6(5.2\varepsilon)^2 \leq 2\varepsilon + 162.3\varepsilon^2 \leq 2.17\varepsilon$$

при $\varepsilon \in (0, 1/960]$.

Повторно воспользуемся леммой 1 (учитывая, что $p \leq 2.17\varepsilon$), по которой функцию f можно реализовать такой схемой S_2 , что при $\varepsilon \in (0, 1/960]$

$$P(S_2) \leq N(S_g)\varepsilon + 6p^2 \leq 2\varepsilon + 6(2.17\varepsilon)^2 \leq 2\varepsilon + 28.3\varepsilon^2 \leq 2.03\varepsilon.$$

Еще раз воспользуемся леммой 1 (учитывая, что $p \leq 2.03\varepsilon$), по которой функцию f можно реализовать такой схемой S_3 , что

$$P(S_3) \leq N(S_g)\varepsilon + 6p^2 \leq 2\varepsilon + 6(2.03\varepsilon)^2 \leq 2\varepsilon + 25\varepsilon^2.$$

Схема $S_3 = C$ искомая. Теорема 10 доказана.

ТЕОРЕМА 11. Пусть полный базис B содержит функцию $\varphi^*(x_1, x_2, x_3)$, конгруэнтную функции вида

$$x_1 \vee x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_2, \sigma_3 \in \{0, 1\},$$

и $B \cap \Psi \neq \emptyset$. Тогда произвольную булеву функцию f в базисе B можно реализовать такой схемой S , что

$$P(S) \leq 2\varepsilon + 25\varepsilon^2$$

при $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Утверждение теоремы следует из теорем 4 и 10.

4. Нижние оценки ненадежности схем. Напомним, что $\tilde{x} = (x_1, x_2, \dots, x_n)$, B_3 – множество всех функций, зависящих от переменных x_1, x_2, x_3 .

Пусть $K_1(n)$ – множество булевых функций $f(x_1, x_2, \dots, x_n)$, $n \geq 3$, не представимых в виде

$$(x_i^a \& h(\tilde{x}))^b \quad \text{или} \quad (x_i^a \& x_j^b \vee x_i^{\bar{a}} \& x_j^{\bar{b}} \& h(\tilde{x}))^c,$$

где $h(\tilde{x})$ – произвольная функция, $i, j \in \{1, 2, \dots, n\}$, $a, b, c \in \{0, 1\}$. Так как

$$|P_2(n) \setminus K_1(n)| \leq 4 \cdot (n2^{2^{n-1}} + (n^2 - n) \cdot 2^{2^{n-2}}),$$

то

$$|K_1(n)| \geq 2^{2^n} - 4 \cdot (n \cdot 2^{2^{n-1}} + (n^2 - n) \cdot 2^{2^{n-2}}).$$

ТЕОРЕМА 12 [9]. Пусть функция $f(\tilde{x}) \in K_1(n)$, а S – любая схема, реализующая функцию f в базисе $B = B_3 \setminus G$. Тогда

$$P(S) \geq 2\varepsilon - 2\varepsilon^2$$

при $\varepsilon \in (0, 1/4]$.

Пусть $K_2(n)$ – множество булевых функций $f(x_1, x_2, \dots, x_n)$, $n \geq 3$, не представимых в виде

$$(x_i^a \& h(\tilde{x}))^b \quad \text{или} \quad ((x_i \oplus x_j)^a \cdot h(\tilde{x}))^b,$$

где $h(\tilde{x})$ – произвольная функция, $i \neq j$, $i, j \in \{1, 2, \dots, n\}$, $a, b \in \{0, 1\}$.

Поскольку

$$|P_2(n) \setminus K_2(n)| \leq 2 \cdot (2n \cdot 2^{2^{n-1}} + (n^2 - n) \cdot (2^{2^{n-2}})^2),$$

то

$$|K_2(n)| \geq 2^{2^n} - (n^2 + n) \cdot 2^{2^{n-1}+1}.$$

УТВЕРЖДЕНИЕ 2 [10]. Пусть функция

$$f(x, y) = \min \left\{ \frac{x}{x+y}, \frac{y}{x+y} \right\}$$

задана в прямоугольнике $D = \{(x, y) \mid a \leq x \leq b, a \leq y \leq b, 0 < a < b\}$. Тогда

$$\max_D f(x, y) = \frac{1}{2}, \quad \min_D f(x, y) = \frac{a}{a+b}.$$

ЛЕММА 17. Пусть f – произвольная отличная от константы функция, а S – такая схема, реализующая f , что $P(S) \leq 5.2\varepsilon$ при всех $\varepsilon \in (0, 1/960]$. Если в схеме S можно выделить подсхему C , которая содержит хотя бы один элемент, имеет один вход и функционирует с ненадежностью $P(C) \leq 3\varepsilon(1 - \varepsilon)^3$, то схема S не является вс-схемой.

ДОКАЗАТЕЛЬСТВО (от противного). Пусть схема S является вс-схемой и C – подсхема схемы S , удовлетворяющая условиям леммы. Очевидно, что подсхема C реализует или тождественную функцию, или инверсию (поскольку f отлична от констант 0, 1). Обозначим через p_0 и p_1 вероятности ошибок на выходе схемы C . Тогда ненадежность схемы C равна $P(C) = \max\{p_0, p_1\}$ и по условию $P(C) \leq 3\varepsilon(1 - \varepsilon)^3$.

Нетрудно проверить, что $p_0, p_1 \geq \varepsilon$. Следовательно, для вероятностей p_0 и p_1 верно неравенство $\varepsilon \leq p_0, p_1 \leq 3\varepsilon(1 - \varepsilon)^3$. По утверждению 2 имеем

$$\frac{1}{4} < \frac{\varepsilon}{\varepsilon + 3\varepsilon(1 - \varepsilon)^3} \leq \min \left\{ \frac{p_0}{p_0 + p_1}, \frac{p_1}{p_0 + p_1} \right\}.$$

С другой стороны, по теореме 6 верно неравенство

$$\min \left\{ \frac{p_0}{p_0 + p_1}, \frac{p_1}{p_0 + p_1} \right\} \leq P(S).$$

Поэтому

$$\frac{1}{4} < \min \left\{ \frac{p_0}{p_0 + p_1}, \frac{p_1}{p_0 + p_1} \right\} \leq P(S) \leq 5.2\varepsilon,$$

т.е. $1/4 < 5.2\varepsilon$, что неверно при $\varepsilon \in (0, 1/960]$.

Лемма 17 доказана.

Пусть S_1 – произвольная схема, содержащая хотя бы один элемент. Функциональный элемент, выход которого является выходом схемы S_1 , будем называть *выходным* элементом схемы S_1 .

ТЕОРЕМА 13. Пусть базис $B \subseteq (\Theta \cup \Theta^* \cup \{\bar{x}_1, 0, 1\})$ или $B \subseteq (\Psi \cup \{\bar{x}_1, 0, 1\})$ или $B \subseteq (\Psi^* \cup \{\bar{x}_1, 0, 1\})$. Если функция $f(\bar{x}) \in K_2(n)$, а S – любая схема, реализующая функцию f в базисе B , то

$$P(S) \geq 3\varepsilon(1 - \varepsilon)^3$$

при $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Пусть B – любой из базисов, удовлетворяющих условию теоремы, функция $f(\tilde{x}) \in K_2(n)$, а S – любая схема, реализующая функцию f . Заметим, что схема S в этом случае содержит не менее трех элементов. Без ограничения общности схему S можно считать вс-схемой.

Рассмотрим всевозможные подсхемы схемы S , содержащие хотя бы один элемент. Возможны два варианта: либо найдется подсхема, которая имеет один вход (обозначим ее через C), либо в схеме S такой подсхемы нет.

1. Допустим, что в схеме S есть подсхема C , которая имеет один вход. Очевидно, что подсхема C реализует или тождественную функцию, или инверсию (поскольку $f(\tilde{x}) \in K_2(n)$ и $0, 1 \notin K_2(n)$). Обозначим через p_0 и p_1 вероятности ошибок на выходе схемы C . Тогда ненадежность схемы C равна $P(C) = \max\{p_0, p_1\}$. Возможны два варианта.

Случай 1.1. Ненадежность $P(C)$ схемы C удовлетворяет следующему неравенству: $P(C) > 3\varepsilon(1 - \varepsilon)^3$. Тогда либо $p_0 > 3\varepsilon(1 - \varepsilon)^3$, либо $p_1 > 3\varepsilon(1 - \varepsilon)^3$, и по теореме 5 получаем неравенство $P(S) > 3\varepsilon(1 - \varepsilon)^3$.

Случай 1.2. Ненадежность схемы C удовлетворяет следующему неравенству: $P(C) \leq 3\varepsilon(1 - \varepsilon)^3$. Применима лемма 17, по которой схема S не является вс-схемой, что неверно.

2. Допустим, что в схеме S нельзя выделить подсхему, содержащую хотя бы один элемент и имеющую ровно один вход. В этом случае доказательство теоремы проводится в зависимости от рассматриваемого базиса, в каждом из подслучаев отдельно. При этом всякий раз будем выделять подсхему (обозначим ее через A) из трех или четырех элементов (в зависимости от функции, приписанной выходному элементу) и применять теорему 5. Введем необходимые обозначения для схемы A .

Обозначим через $p_{11}, \dots, p_{1r}$ всевозможные различные вероятности ошибок на выходе схемы A при нулевых входных наборах схемы A . Аналогично, пусть $p_{01}, \dots, p_{0t}$ – всевозможные различные вероятности ошибок на выходе схемы A при единичных входных наборах схемы A . Полагаем

$$p^1 = \min\{p_{11}, \dots, p_{1r}\}, \quad p^0 = \min\{p_{01}, \dots, p_{0t}\}.$$

Обозначим через E_1 выходной элемент схемы S (и подсхемы A).

Случай 2.1. Пусть базис $B = \Theta \cup \Theta^* \cup \{\bar{x}_1, 0, 1\}$. Возможны следующие варианты.

Подслучай 2.1.1. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная одной из функций вида

$$x_1^{\sigma_1} x_2^{\sigma_2}, \quad x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\},$$

и никакие два входа элемента E_1 не отождествлены. Тогда в схеме S найдутся такие два различных элемента E_2 и E_3 , что их выходы соединены со входами элемента E_1 (поскольку схема S реализует функцию $f \in K_2(n)$, ни один вход элемента E_1 не может быть соединен с полюсом схемы S). Не ограничивая общности, в этом случае будем считать, что выход элемента E_2 соединен с первым входом элемента E_1 и выход элемента E_3 соединен со вторым входом элемента E_1 . Обозначим через A подсхему, состоящую из элементов E_1, E_2, E_3 . Заметим, что функция e_1 имеет ровно один единичный набор. Оценим вероятность ошибки p^0 схемы A на единичном

входном наборе. Пусть при поступлении единичного набора на вход схемы A ошибается только элемент E_1 , тогда на выходе всей схемы вместо 1 появится 0. Пусть при поступлении единичного набора на вход схемы A ошибается элемент E_2 или E_3 , тогда на вход элемента E_1 поступит набор, отличный от единичного набора функции e_1 , и на выходе всей схемы вместо 1 появится 0. Таким образом, при ошибке в точности одного элемента в схеме A на единичном входном наборе на выходе схемы вместо 1 появится 0. Поэтому

$$p^0 \geq \varepsilon(1 - \varepsilon)^2 + \varepsilon(1 - \varepsilon)^2 + \varepsilon(1 - \varepsilon)^2 = 3\varepsilon(1 - \varepsilon)^2 > 3\varepsilon(1 - \varepsilon)^3.$$

Тогда по теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

Подслучай 2.1.2. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная одной из функций вида

$$x_1^{\sigma_1} \vee x_2^{\sigma_2}, \quad x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee x_3^{\sigma_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\},$$

и ни одна пара входов элемента E_1 не отождествлена. Тогда, используя результат пункта 2.1.1 и применяя теорему 4, получаем неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

Подслучай 2.1.3. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная функции вида

$$x_1^{\sigma_1}(x_2 \oplus x_3)^{\sigma_2}, \quad \sigma_1, \sigma_2 \in \{0, 1\},$$

и никакие два входа элемента E_1 не отождествлены. Тогда в схеме S найдутся такие два различных элемента E_2 и E_3 , что выход элемента E_2 соединен с первым входом элемента E_1 , а выход элемента E_3 соединен со вторым или третьим входом элемента E_1 (поскольку схема S реализует функцию $f \in K_2(n)$, первый и второй или первый и третий входы элемента E_1 не могут быть соединены с полюсами схемы S). Не ограничивая общности, в этом случае будем считать, что выход элемента E_3 соединен со вторым входом элемента E_1 . Обозначим через A подсхему, состоящую из элементов E_1, E_2, E_3 . Заметим, что функция e_1 имеет ровно два единичных набора. Оценим вероятности ошибок схемы A на этих наборах.

Пусть при поступлении единичного набора на вход схемы A ошибается только элемент E_1 , тогда на выходе всей схемы вместо 1 появится 0. Пусть при поступлении единичного набора на вход схемы A ошибается элемент E_2 или E_3 , тогда на вход элемента E_1 поступит набор, отличный от единичного набора функции e_1 , и на выходе всей схемы вместо 1 появится 0. Таким образом, при ошибке в точности одного элемента в схеме A на единичных входных наборах на выходе схемы вместо 1 появится 0. Поэтому

$$p^0 \geq \varepsilon(1 - \varepsilon)^2 + \varepsilon(1 - \varepsilon)^2 + \varepsilon(1 - \varepsilon)^2 = 3\varepsilon(1 - \varepsilon)^2 > 3\varepsilon(1 - \varepsilon)^3.$$

Тогда по теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

Подслучай 2.1.4. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная функции вида

$$x_1^{\sigma_1} \vee (x_2 \oplus x_3)^{\sigma_2}, \quad \sigma_1, \sigma_2 \in \{0, 1\},$$

и никакие два входа элемента E_1 не отождествлены. Тогда, используя результат пункта 2.1.3 и применяя теорему 4, получаем неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^2$.

Подслучай 2.1.5. Пусть выходному элементу E_1 приписана функция e_1 , равная константе 0 или 1. В этом случае вся схема S реализует константу 0 или 1, что противоречит выбору функции f .

Подслучай 2.1.6. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная одной из функций вида

$$x_1^a x_2^b x_3^c, \quad x_1^a \vee x_2^b \vee x_3^c, \quad x_1^a (x_2 \oplus x_3)^b, \quad x_1^a \vee (x_2 \oplus x_3)^b, \quad a, b, c \in \{0, 1\},$$

и некоторые два входа элемента E_1 отождествлены. В этом случае выходной элемент E_1 будет функционировать как элемент, реализующий либо константу, либо функцию конгруэнтную функции вида

$$x_1^a x_2^b, \quad x_1^a \vee x_2^b, \quad a, b \in \{0, 1\}.$$

Эти случаи рассмотрены в предыдущих пунктах доказательства.

Таким образом, в базисе $B = \Theta \cup \Theta^* \cup \{\bar{x}_1, 0, 1\}$ утверждение теоремы верно. Очевидно, что оно верно в любом полном базисе $B \subseteq (\Theta \cup \Theta^* \cup \{\bar{x}_1, 0, 1\})$.

Случай 2.2. Рассмотрим базис $B = \Psi \cup \{\bar{x}_1, 0, 1\}$. Возможны следующие варианты.

Подслучай 2.2.1. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная функции вида

$$x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}), \quad \sigma_2, \sigma_3 \in \{0, 1\},$$

и никакие два входа элемента E_1 не отождествлены. Поскольку схема S реализует функцию $f \in K_2(n)$, первый вход элемента E_1 не может быть соединен с полюсом схемы S , поэтому в схеме S найдется такой элемент E_2 , что его выход соединен с первым входом элемента E_1 . Возможны следующие варианты:

1) Пусть элементу E_2 приписана константа 0. В этом случае схема S реализует константу 0, что невозможно, поскольку $f \in K_2(n)$.

2) Пусть элементу E_2 приписана константа 1. В этом случае второй и третий входы элемента E_1 не могут быть соединены с полюсами схемы S ($f \in K_2(n)$), поэтому в схеме S найдутся различные элементы E_3 и E_4 , выходы которых соединены со вторым и третьим входами элемента E_1 соответственно. Обозначим через A подсхему, состоящую из элементов E_1, E_2, E_3, E_4 . Тогда на всех нулевых наборах схемы A при ошибке только одного из элементов E_1, E_3, E_4 на выходе схемы A вместо 0 появится 1. Поэтому $p^1 \geq 3\varepsilon(1 - \varepsilon)^3$. По теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

3) Пусть элементу E_2 приписана функция e_2 , конгруэнтная одной из функций вида

$$x_1^{\sigma_1} x_2^{\sigma_2}, \quad x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3}, \quad \sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}.$$

В этом случае в схеме S найдется элемент E_3 , выход которого соединен с одним из входов элемента E_2 . Тогда на всех единичных наборах подсхемы A , состоящей из элементов E_1, E_2, E_3 , при ошибке ровно одного элемента E_1, E_2 или E_3 на

выходе схемы A вместо 1 появится 0. Поэтому $p^0 \geq 3\varepsilon(1 - \varepsilon)^2$. По теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^2$.

4) Пусть элементу E_2 приписана функция e_2 , конгруэнтная функции вида

$$x_1^{\sigma_1}(x_2 \oplus x_3)^{\sigma_2}, \quad \sigma_1, \sigma_2 \in \{0, 1\}.$$

В этом случае в схеме S существует элемент E_3 , выход которого соединен с первым входом элемента E_2 . Заметим, что элементу E_3 приписана функция e_3 , отличная от константы 0 (иначе $f \notin K_2(n)$). Тогда на всех единичных наборах подсхемы A , состоящей из элементов E_1, E_2, E_3 , при ошибке ровно одного элемента E_1, E_2 или E_3 на выходе схемы A вместо 1 появится 0. Поэтому $p^0 \geq 3\varepsilon(1 - \varepsilon)^2$. По теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^2$.

5) Пусть элементу E_2 приписана функция e_2 , конгруэнтная функции вида

$$x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}), \quad \sigma_2, \sigma_3 \in \{0, 1\}.$$

В этом случае в схеме S существует элемент E_3 , выход которого соединен с первым входом элемента E_2 . Заметим, что элементу E_3 приписана функция e_3 , отличная от константы 0 (иначе $f \notin K_2(n)$). Тогда на всех единичных наборах подсхемы A , состоящей из элементов E_1, E_2, E_3 , при ошибке ровно одного элемента E_1, E_2 или E_3 на выходе схемы A , состоящей из элементов E_1, E_2, E_3 , вместо 1 появится 0. Поэтому $p^0 \geq 3\varepsilon(1 - \varepsilon)^2 \geq 3\varepsilon(1 - \varepsilon)^3$. По теореме 5 верно неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

Подслучай 2.2.2. Пусть выходному элементу E_1 приписана функция e_1 , конгруэнтная функции вида

$$x_1(x_2^a \vee x_3^b), \quad a, b \in \{0, 1\},$$

и некоторые два входа элемента E_1 отождествлены. В этом случае элемент E_1 реализует либо тождественную функцию, либо функцию конгруэнтную функции вида $x_1^a x_2^b$, $a, b \in \{0, 1\}$. Эти ситуации рассмотрены в случае 1 и подслучае 2.1.1 доказательства.

Подслучай 2.2.3. Остальные варианты для функций, приписанных элементу E_1 , полностью совпадают с рассмотренными в подслучаях 2.1.1, 2.1.3, 2.1.5 и 2.1.6 доказательства.

Таким образом, в базисе $B = \Psi \cup \{\bar{x}_1, 0, 1\}$ утверждение теоремы верно. Очевидно, что оно верно в любом полном базисе $B \subseteq (\Psi \cup \{\bar{x}_1, 0, 1\})$.

Случай 2.3. Рассмотрим базис $B = \Psi^* \cup \{\bar{x}_1, 0, 1\}$. Учитывая результаты случая 2.2 и применяя теорему 4, получаем неравенство $P(S) \geq 3\varepsilon(1 - \varepsilon)^3$.

Теорема 13 доказана.

5. Выводы. Из теоремы 7 следует, что если в полном базисе B содержится функция из множества M , то любую булеву функцию в этом базисе можно реализовать схемой S , ненадежность которой $P(S) \leq 2\varepsilon + 79\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Из теоремы 8 следует, что если полный базис $B \subseteq (\hat{\Psi} \cup M_5)$ и $B \cap M_5 \neq \emptyset$, то любую булеву функцию в этом базисе можно реализовать такой схемой S , что $P(S) \leq 2\varepsilon + 65\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$. Напомним, что $\hat{\Psi} = B_3 \setminus (G \cup M \cup M_5)$.

Из теоремы 9 следует, что если полный базис B содержит линейную функцию, существенно зависящую не менее чем от двух переменных, то любую булеву функцию в этом базисе можно реализовать такой схемой S , что $P(S) \leq 2\varepsilon + 65\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Из теорем 10 и 11 следует, что если полный базис $B \subseteq \tilde{\Psi}$ удовлетворяет хотя бы одному из следующих условий:

- 1) базис B содержит функцию $\varphi(x_1, x_2, x_3)$, конгруэнтную функции вида

$$x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}), \quad \sigma_2, \sigma_3 \in \{0, 1\},$$

и $B \cap \Psi^* \neq \emptyset$;

- 2) базис B содержит функцию $\varphi^*(x_1, x_2, x_3)$, конгруэнтную функции вида

$$x_1 \vee x_2^{\sigma_2} x_3^{\sigma_3},$$

и $B \cap \Psi \neq \emptyset$,

то любую булеву функцию в базисе B можно реализовать такой схемой S , что $P(S) \leq 2\varepsilon + 25\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Итак, из теорем 7–11 следует, что базис B , удовлетворяющий условиям хотя бы одной из них, имеет коэффициент ненадежности не больше 2. Если же базис не только удовлетворяет условиям теорем 7–11, но и еще двум условиям $B \subseteq B_3$ и $B \cap G = \emptyset$, то его коэффициент ненадежности не меньше 2 (см. теорему 12). Таким образом, если базис $B \subseteq B_3$, $B \cap G = \emptyset$ и удовлетворяет условиям хотя бы одной из теорем 7–11, то его коэффициент ненадежности равен 2. Отметим также, что в этом базисе для почти всех функций (поскольку $|K_1(n)|/2^{2^n} \rightarrow 1$ с ростом n) асимптотически оптимальные по надежности схемы функционируют с ненадежностью, асимптотически равной 2ε , $\varepsilon \rightarrow 0$.

Из теоремы 13 следует, что если полный базис $B \subseteq \tilde{\Psi}$ не удовлетворяет условиям теорем 10, 11, то его коэффициент ненадежности не меньше 3. Следовательно, в B_3 нет других полных базисов B с коэффициентом ненадежности 2, кроме тех, для которых $B \cap G = \emptyset$ и выполняются условия хотя бы одной из теорем 7–11.

Таким образом, получаем следующий результат: полный базис $B \subseteq B_3$ имеет коэффициент ненадежности 2 тогда и только тогда, когда $B \cap G = \emptyset$ и выполнены условия хотя бы одной из теорем 7, 8, 10 и 11.

Эти результаты сформулированы во введении (теорема 0).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] О. Б. Лупанов, *Асимптотические оценки сложности управляющих систем*, Изд-во Моск. ун-та, М., 1984.
- [2] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components", *Automata Studies*, Ann. of Math. Stud., **34**, Princeton Univ. Press, Princeton, NJ, 1956, 43–98.
- [3] С. И. Ортюков, "Об избыточности реализации булевых функций схемами из ненадежных элементов", *Труды семинара по дискретной математике и ее приложениям* (Москва, 27–29 января 1987 г.), Изд-во Моск. ун-та, М., 1989, 166–168.
- [4] D. Uhlig, "Reliable networks from unreliable gates with almost minimal complexity", *Fundamentals of Computation Theory. Intern. conf. FCT'87* (Kazan, June 1987), Lecture Notes in Comput. Sci., **278**, Springer-Verl., Proc. Berlin, 1987, 462–469.

- [5] С. В. Яблонский, “Асимптотически наилучший метод синтеза надежных схем из ненадежных элементов”, *Discrete Mathematics, Banach Cent. Publ.*, **7**, PWN, Warsaw, 1982, 11–19.
- [6] М. А. Алехина, *Синтез асимптотически оптимальных по надежности схем из ненадежных элементов*, ИИЦ ПГУ, Пенза, 2006.
- [7] В. В. Чугунова, *Синтез асимптотически оптимальных по надежности схем при инверсных неисправностях на входах элементов*, Дисс. ... канд. физ.-матем. наук, Пенза, 2007.
- [8] С. И. Аксенов, “О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов”, *Изв. вузов. Поволжский регион. Естественные науки*, 2005, № 6(21), 42–55.
- [9] М. А. Алехина, А. В. Васин, “О надежности схем в базисах, содержащих функции не более чем трех переменных”, *Физико-математические науки*, Учен. зап. Казан. гос. ун-та. Сер. Физ.-матем. науки, **151**, № 2, Изд-во Казанского ун-та, Казань, 2009, 25–35.
- [10] А. В. Васин, “Об асимптотически оптимальных схемах в базисе $\{\&, \neg\}$ при инверсных неисправностях на выходах элементов”, *Дискретн. анализ и исслед. опер.*, **16**:6 (2009), 12–22.
- [11] А. В. Васин, “О функциях специального вида”, *Труды VIII Международной конференции “Дискретные модели в теории управляющих систем”* (Лесной городок Моск. обл., 6–9 апреля 2009 г.), МАКС Пресс, М., 2009, 43–46.
- [12] М. А. Алехина, С. И. Аксенов, А. В. Васин, “О функциях и схемах, применяемых для повышения надежности схем”, *Изв. вузов. Поволжский регион. Физ.-матем. науки*, 2008, № 3, 30–38.
- [13] Н. П. Редькин, “О полных проверяющих тестах”, *Математические вопросы кибернетики*, **2**, Физматлит, 1989, 198–222.
- [14] М. А. Алехина, П. Г. Пичугина, “О надежности двойственных схем в полном конечном базисе”, *Синтез и сложность управляющих систем*, Материалы XVIII Международной школы-семинара им. О. Б. Лупанова (г. Пенза 28 сентября–3 октября 2009 г.), Изд-во мех.-мат. ф-та МГУ, М., 2009, 10–13.
- [15] А. В. Васин, “О базисах, в которых асимптотически оптимальные схемы имеют ненадежность 2ε ”, *Материалы X Международного семинара “Дискретная математика и ее приложения”* (г. Москва, 1–6 февраля 2010 г.), Изд-во мех.-мат. ф-та МГУ, М., 2010, 94–97.
- [16] М. А. Алехина, А. В. Васин, “Достаточные условия реализации булевых функций асимптотически оптимальными схемами с ненадежностью 2ε ”, *Изв. вузов. Матем.*, 2010, № 5, 79–82.
- [17] А. В. Васин, “О надежности схем в полных конечных базисах, содержащих линейную функцию”, *Труды международного симпозиума “Надежность и качество, 2010”*, Т. 1 (г. Пенза, 24–31 мая 2010 г.), ИИЦ ПГУ, Пенза, 2010, 241–242.
- [18] А. В. Васин, *Асимптотически оптимальные по надежности схемы в полных базисах из трехходовых элементов*, Дисс. ... канд. физ.-матем. наук, Пенза, 2010.

М. А. Алехина

Пензенский государственный университет

E-mail: ama@sura.ru

Поступило

30.03.2010

Исправленный вариант

30.01.2013

А. В. Васин

Пензенский государственный университет

E-mail: alvarvasin@mail.ru