ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Ноябрь—декабрь 2013. Том 20, № 6. С. 3–15

УДК 519.718

АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫЕ ПО НАДЁЖНОСТИ СХЕМЫ В НЕКОТОРЫХ БАЗИСАХ *)

А. В. Васин

Аннотация. Рассматривается реализация булевых функций схемами из ненадёжных 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. Найдены все базисы, в которых почти все булевы функции можно реализовать асимптотически оптимальными по надёжности схемами, функционирующими с ненадёжностью 3ε при $\varepsilon \to 0$. Доказано, что других таких базисов $B \subset B_3$ нет.

Ключевые слова: ненадёжный функциональный элемент, асимптотически оптимальная по надёжности схема, инверсная неисправность на выходах элементов, синтез схемы из ненадёжных элементов.

Введение

Рассматривается реализация булевых функций схемами из ненадёжных функциональных элементов в полном конечном базисе B. Предполагается, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0; 1/2)$ подвержены инверсным неисправностям на выходах [9]. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию e, а в неисправном — функцию $\overline{e}$.

Считаем, что схема S из ненадёжных элементов реализует булеву функцию $f(x_1, x_2, \ldots, x_n)$, если при поступлении на входы схемы набора $\widetilde{a} = (a_1, a_2, \ldots, a_n)$ при отсутствии неисправностей в схеме на её выходе появляется значение $f(\widetilde{a})$. Обозначим через $P_{\overline{f(\widetilde{a})}}(S, \widetilde{a})$ вероятность ошибки на входном наборе $\widetilde{a}$ схемы S, реализующей функцию f. Число $P(S) = \max\limits_{\widetilde{a}} P_{\overline{f(\widetilde{a})}}(S, \widetilde{a})$ назовём *ненадёжностью схемы* S. Надёжность схемы S равна $1 - P(S)$.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 11–01–00212).

Пусть $P_\varepsilon(f) = \inf\limits_S P(S)$, где ε — вероятность инверсной неисправности на выходе одного элемента, а инфимум берётся по всем схемам S из ненадёжных элементов, реализующим функцию $f(x_1, x_2, \ldots, x_n)$. Схема A из ненадёжных элементов, реализующая функцию f, называется *асимптотически оптимальной по надёжности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е.

$$\lim_{\varepsilon \to 0} \frac{P_\varepsilon(f)}{P(A)} = 1.$$

В [3, 6] найдено множество функций $G = G_1 \cup G_2 \cup G_3$, зависящих от переменных x_1, x_2 и x_3, где G_1, G_2 и G_3 — множества функций, конгруэнтных функциям $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}$, $x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3}$ и $x_1^{\sigma_1}x_2^{\overline{\sigma}_2} \vee x_2^{\sigma_2}x_3^{\sigma_3}$ соответственно, $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$. Множество G содержит 56 функций. Наличия в базисе любой из этих функций достаточно для того, чтобы произвольную булеву функцию можно было реализовать схемой с ненадёжностью, асимптотически равной ε, где ε — вероятность инверсной неисправности на выходе одного элемента в схеме.

Обозначим через B_3 множество всех булевых функций, зависящих от переменных x_1, x_2, x_3.

Нами найдены базисы $B \subset B_3$, в которых почти все булевы функции можно реализовать асимптотически оптимальными по надёжности схемами, функционирующими с ненадёжностью 3ε при $\varepsilon \to 0$, и показано, что в других базисах $B \subset B_3$ для почти всех функций любая схема функционирует с ненадёжностью не меньше $4\varepsilon(1-\varepsilon)^3$ при $\varepsilon \in (0, 1/960]$.

Обозначим через G_4 множество функций, зависящих от переменных x_1, x_2, x_3, x_4 и конгруэнтных функциям $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_3^{\sigma_3}x_4^{\sigma_4}$ или $\left(x_1^{\sigma_1} \vee x_2^{\sigma_2}\right)\left(x_3^{\sigma_1} \vee x_4^{\sigma_4}\right)$, где $\sigma_i \in \{0, 1\}$, $i = 1, 2, 3, 4$.

Теорема 1 [1]. *Допустим, что любую функцию можно реализовать схемой с ненадёжностью не больше p ($p \leqslant 1/2$). Пусть схема S_g реализует функцию $g \in G_1 \cup G_4$ с ненадёжностью $P(S_g)$, причём v^1 и v^0 — вероятности ошибок схемы S_g на наборах $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_i)$ и $(\sigma_1, \sigma_2, \sigma_i)$ соответственно, если g зависит от i переменных, $i = 3, 4$. Тогда произвольную функцию $f(x_1, \ldots, x_n)$ можно реализовать схемой S такой, что*

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

Лемма 1 [4]. *Пусть схема S_φ реализует функцию $\varphi \in G_2$, т. е. функцию вида $x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3}$ ($\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$) с ненадёжностью $P(S_\varphi) = p_\varphi$.*

Тогда можно построить схему S_g, реализующую функцию $g = x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3} \in G_1$, такую, что $P(S_g) \leqslant p_\varphi + 2p_\oplus$ ($p_\oplus$ — максимальная из ненадёжностей 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 $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3)$ и $(\sigma_1, \sigma_2, \sigma_3)$ соответственно выполняются неравенства $v^1, v^0 \leqslant p_\varphi + 2p_\varphi p_\oplus + p_\oplus^2$.

Теорема 2 [3]. *При $\varepsilon \leqslant 1/960$ любую функцию f в произвольном полном конечном базисе можно реализовать схемой A с ненадёжностью $P(A) \leqslant 5\varepsilon + 182\varepsilon^2 \leqslant 5{,}2\varepsilon$.*

Пусть E — функциональный элемент, которому приписана функция $e(x_1, x_2, \ldots, x_m)$, $m \in N$. Элемент E^* с приписанной ему функцией $e^*(x_1, x_2, \ldots, x_m)$, двойственной функции $e(x_1, x_2, \ldots, x_m)$, называется *двойственным элементу E*, если для любого входного набора $(b_1, b_2, \ldots, b_m)$ для вероятностей ошибок верно равенство

$$P_{\overline{e}(b_1,b_2,\ldots,b_m)}(E, (b_1, b_2, \ldots, b_m)) = P_{\overline{e}^*(\overline{b}_1,\overline{b}_2,\ldots,\overline{b}_m)}(E^*, (\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_m)).$$

Две схемы S и S^* назовём *двойственными*, если одна получается из другой заменой всех элементов двойственными.

Теорема 3 [5]. *Для любых двойственных схем S и S^* верно равенство $P(S) = P(S^*)$.*

Теорема 4 [1]. *Пусть f — произвольная булева функция, отличная от константы, S — любая схема, её реализующая. Пусть подсхема C схемы S содержит выход схемы S и реализует булеву функцию h с ненадёжностью $P(C) \leqslant 1/2$. Обозначим через $p_{11}, \ldots, p_{1k}$ всевозможные различные вероятности ошибок на выходе схемы C при нулевых входных наборах $\widetilde{b}$, т. е. $h(\widetilde{b}) = 0$. Аналогично, пусть $p_{01}, \ldots, p_{0m}$ — всевозможные различные вероятности ошибок на выходе схемы C при единичных входных наборах $\widetilde{b}$, т. е. $h(\widetilde{b}) = 1$. Полагаем $p^1 = \min\{p_{11}, \ldots, p_{1k}\}$, $p^0 = \min\{p_{01}, \ldots, p_{0m}\}$. Тогда вероятности ошибок на выходе схемы S удовлетворяют неравенствам $P_1(S, \widetilde{a}) \geqslant p^1$, если $f(\widetilde{a}) = 0$; $P_0(S, \widetilde{a}) \geqslant p^0$, если $f(\widetilde{a}) = 1$.*

Следствие 1 [1]. $P(S) \geqslant \max\{p^0, p^1\}$.

Пусть в схеме, реализующей булеву функцию, отличную от константы, выделена подсхема A с одним входом и выходом схемы. Обозначим через S' подсхему, получаемую из схемы S удалением A. Если выполнено неравенство $P(S) > P(S')$, то будем говорить, что схема S' *надёжнее* схемы S и получается из S удалением подсхемы A.

Так как схема S реализует функцию, отличную от константы, схема A реализует либо тождественную функцию, либо инверсию.

Схема S, реализующая функцию f, отличную от константы, является *bc-схемой*, если из неё нельзя получить более надёжную схему, реализующую f или $\overline{f}$, удалением подсхемы, реализующей тождественную функцию или инверсию.

Теорема 5 [1]. *Пусть схема S с ненадёжностью $P(S)$ реализует функцию f и является bc-схемой. Если в S можно выделить подсхему, имеющую один вход, содержащую выход схемы 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*

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

1. Верхние оценки ненадёжности схем

Обозначим через Ψ множество функций, зависящих от переменных x_1, x_2, x_3, и конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2}$, $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}$, $x_1^{\sigma_1}\bigl(x_2^{\sigma_2}x_3^{\sigma_3} \vee x_2^{\overline{\sigma}_2}x_3^{\overline{\sigma}_3}\bigr)$, $x_1\bigl(x_2^{\sigma_2} \vee x_3^{\sigma_3}\bigr)$ $(\sigma_1, \sigma_2, \sigma_3 \in \{0,1\})$, через Ψ^* — множество функций, двойственных функциям множества Ψ, через Θ — множество функций, зависящих от переменных x_1, x_2, x_3, конгруэнтных функциям $x_1^a x_2^b$, $x_1^a x_2^b x_3^c$, $x_1^a(x_2 \oplus x_3)^b$, где $a, b, c \in \{0,1\}$, через Θ^* — множество функций, двойственных функциям множества Θ, через H — множество функций $\{\overline{x}_1\overline{x}_2\overline{x}_3,\ \overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3,\ \overline{x}_1(\overline{x}_2\overline{x}_3 \vee x_2x_3),\ \overline{x}_1 \vee (x_2\overline{x}_3 \vee \overline{x}_2x_3)\}$.

Теорема 6 [2]. *Пусть $B = \{\overline{x}_1 \vee \overline{x}_2\}$ или $B = \{\overline{x}_1\overline{x}_2\}$. Тогда произвольную булеву функцию f в базисе B можно реализовать схемой S такой, что $P(S) \leqslant 3\varepsilon + 126\varepsilon^2$ при любом $\varepsilon \in (0, 1/600]$.*

Теорема 7. *Пусть полный конечный базис B содержит хотя бы одну из функций множества H и либо $B \subset (\Theta \cup \Theta^* \cup \{\overline{x}_1, 0, 1\})$, либо $B \subset (\Psi \cup \{\overline{x}_1, 0, 1\})$, либо $B \subset (\Psi^* \cup \{\overline{x}_1, 0, 1\})$. Тогда произвольную булеву функцию f в базисе B можно реализовать схемой S такой, что $P(S) \leqslant 3\varepsilon + 126\varepsilon^2$ при любом $\varepsilon \in (0, 1/600]$.*

Доказательство. Утверждение теоремы следует из теоремы 6, так как из любой функции множества H отождествлением некоторых двух переменных можно получить функцию, конгруэнтную $\overline{x}_1 \vee \overline{x}_2$ или $\overline{x}_1\overline{x}_2$.

Лемма 2 [7]. *Пусть $\varphi \in \Psi$. Тогда отождествлением переменных из φ можно получить функцию вида $x_1^a x_2^b$, $a, b \in \{0,1\}$.*

Лемма 3 [7]. *Пусть $\varphi \in \Psi^*$. Тогда отождествлением переменных из φ можно получить функцию вида $x_1^a \vee x_2^b$, $a, b \in \{0,1\}$.*

Теорема 8. *Пусть полный конечный базис B содержит функции $\varphi_1 \in \Theta$ и $\varphi_2 \in \Theta^*$. Тогда произвольную булеву функцию f в базисе B можно реализовать схемой S такой, что $P(S) \leqslant 3\varepsilon + 225\varepsilon^2$ при любом $\varepsilon \in (0, 1/960]$.*

Доказательство. Пусть полный конечный базис B содержит функции $\varphi_1 \in \Theta$ и $\varphi_2 \in \Theta^*$. По лемме 2 из функции $\varphi_1 \in \Theta$ отождествлением переменных можно получить функцию $\varphi_1'(z_1, z_2) = z_1^a z_2^b$, $a, b \in \{0,1\}$, а по лемме 3 из функции $\varphi_2 \in \Theta^*$ отождествлением переменных можно получить функцию $\varphi_2'(z_1, z_2) = z_1^c \vee z_2^d$, $c, d \in \{0,1\}$. Тогда, моделируя формулу $\varphi_1'(\varphi_i'(z_1, z_2), \varphi_j'(z_3, z_4))$ ($i = 1$, если $a = 1$; $i = 2$, если $a = 0$; $j = 1$, если $b = 1$; $j = 2$, если $b = 0$), построим схему S_g из 3-х элементов, реализующую функцию $g = \big(z_1^{\sigma_1} \vee z_2^{\sigma_2}\big)\big(z_3^{\sigma_3} \vee z_4^{\sigma_4}\big) \in G_4$ ($\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in \{0,1\}$). Так как схема S_g содержит ровно 3 элемента, имеем $P(S_g) \leqslant 3\varepsilon$.

По теореме 2 при $\varepsilon \leqslant 1/960$ любую булеву функцию f можно реализовать схемой A такой, что $P(A) \leqslant 5{,}2\varepsilon$. Применяя теорему 1, по схеме A построим реализующую функцию f схему S такую, что

$$P(S) \leqslant 3\varepsilon + 4 \cdot 5{,}2\varepsilon \cdot 3\varepsilon + 6(5{,}2\varepsilon)^2 \leqslant 3\varepsilon + 225\varepsilon^2.$$

Теорема 8 доказана.

Теорема 9. *Пусть полный базис $B \subset (\Psi \cup \{\overline{x}, 0, 1\})\backslash H$ удовлетворяет хотя бы одному из следующих условий*:

(i) *B содержит функцию, конгруэнтную $\varphi = x_1\big(x_2^{\sigma_2} \vee x_3^{\sigma_3}\big)$, $\sigma_2, \sigma_3 \in \{0,1\}$;*

(ii) *B содержит константу 1 и функцию, конгруэнтную $\varphi = x_1\big(x_2 \oplus x_3 \oplus \sigma_3\big)$, $\sigma_3 \in \{0,1\}$;*

(iii) *B содержит функцию, конгруэнтную $\varphi = \overline{x}_1(x_2 \oplus x_3)$.*

Тогда произвольную булеву функцию f в базисе B можно реализовать схемой S такой, что $P(S) \leqslant 3\varepsilon + 293\varepsilon^2$ при любом $\varepsilon \in (0, 1/960]$.

Доказательство. Пусть $\varepsilon \in (0, 1/960]$ и $B \subset (\Psi \cup \{\overline{x}, 0, 1\})\backslash H$ — полный базис. По лемме 2 из функции $\varphi \in \Psi$ отождествлением переменных можно получить функцию $\varphi'(z_1, z_2) = z_1^a z_2^b$, $a, b \in \{0,1\}$. Заметим, что все функции множества $(\Psi \cup \{\overline{x}, 0, 1\})\backslash H$ за исключением функций $\overline{x}$ и 1 сохраняют константу 0. Поэтому в полном базисе B содержится хотя бы одна из функций $\overline{x}$ и 1.

Рассмотрим возможные случаи.

(i) Пусть $\varphi = x_1\big(x_2^{\sigma_2} \vee x_3^{\sigma_3}\big)$ $(\sigma_2, \sigma_3 \in \{0,1\})$ принадлежит полному конечному базису B.

(a) Пусть базис B содержит функцию $\overline{x}$. Поскольку

$$\varphi(\overline{\varphi'(z_1, z_2)}, x_2, x_3) = \big(z_1^a \vee z_2^b\big)\big(x_2^{\sigma_2} \vee x_3^{\sigma_3}\big),$$

моделируя формулу $\varphi(\overline{\varphi'(z_1, z_2)}, x_2, x_3)$, построим схему S_g из трёх элементов, реализующую функцию из множества G_4. Ясно, что $P(S_g) \leqslant 3\varepsilon$.

(b) Пусть базис B содержит константу 1. Поскольку

$$\varphi(\varphi(1, x_1, x_2), x_3, x_4) = \big(x_1^{\sigma_2} \vee x_2^{\sigma_3}\big)\big(x_3^{\sigma_2} \vee x_4^{\sigma_3}\big),$$

моделируя формулу $\varphi(\varphi(1, x_1, x_2), x_3, x_4)$, построим схему S_g из трёх элементов, реализующую функцию из множества G_4. Ясно, что $P(S_g) \leqslant 3\varepsilon$.

По теореме 2 при $\varepsilon \leqslant 1/960$ любую булеву функцию f можно реализовать схемой A такой, что $P(A) \leqslant 5{,}2\varepsilon$. Применяя теорему 1, по схеме A построим реализующую функцию f схему S такую, что

$$P(S) \leqslant 3\varepsilon + 4 \cdot 5{,}2\varepsilon \cdot 3\varepsilon + 6(5{,}2\varepsilon)^2 \leqslant 3\varepsilon + 225\varepsilon^2.$$

(ii) Пусть полный конечный базис B содержит константу 1 и функцию, конгруэнтную функции $\varphi = x_1(x_2 \oplus x_3 \oplus \sigma_3)$ $(\sigma_3 \in \{0,1\})$. Поскольку $\varphi(1, \varphi'(z_1, z_2), x_3) = z_1^a z_2^b \oplus x_3 \oplus \sigma_3$, моделируя формулу $\varphi(1, \varphi'(z_1, z_2), x_3)$, построим схему S_φ из трёх элементов, реализующую функцию из множества G_2. Ясно, что $P(S_\varphi) \leqslant 3\varepsilon$. Нетрудно показать, что в базисе B функции $x_2 \oplus x_3$ и $x_2 \oplus x_3 \oplus 1$ можно реализовать схемами S_1 и S_2 соответственно, каждая из которых содержит не более четырёх элементов. Обозначим $P(S_\oplus) = \max\{P(S_1), P(S_2)\}$. Ясно, что $P(S_\oplus) \leqslant 4\varepsilon$. Тогда, применяя лемму 1, построим реализующую функцию $g \in G_1$ схему S_g такую, что $P(S_g) \leqslant 11\varepsilon$, а $v^1, v^0 \leqslant 3\varepsilon + 2 \cdot 3\varepsilon \cdot 4\varepsilon + (4\varepsilon)^2 = 3\varepsilon + 40\varepsilon^2$. По теореме 2 при $\varepsilon \leqslant 1/960$ любую булеву функцию f можно реализовать схемой A такой, что $P(A) \leqslant 5{,}2\varepsilon$. Применяя теорему 1, по схеме A построим реализующую функцию f схему S такую, что

$$P(S) \leqslant 3\varepsilon + 40\varepsilon^2 + 3 \cdot 5{,}2\varepsilon \cdot 11\varepsilon + 3(5{,}2\varepsilon)^2 \leqslant 3\varepsilon + 293\varepsilon^2.$$

(iii) Пусть полный конечный базис B содержит функцию, конгруэнтную $\varphi = \overline{x}_1(x_2 \oplus x_3)$. Поскольку $\varphi(x_2, x_2, x_2) \equiv 0$, константу 0 можно реализовать, используя один функциональный элемент. Нетрудно видеть, что $\varphi(0, \varphi'(z_1, z_2), x_3) = \overline{0}\big(z_1^a z_2^b \oplus x_3\big)$. Поэтому моделируя формулу

$\varphi(0, \varphi'(z_1, z_2), x_3)$, построим схему S_φ из трёх элементов, реализующую функцию из множества G_2. Ясно, что $P(S_\varphi) \leqslant 3\varepsilon$.

(a) Пусть базис B содержит функцию $\overline{x}$. Нетрудно проверить, что $\varphi(0, x_2, x_3) = x_2 \oplus x_3$ и $\varphi(0, \overline{x}_2, x_3) = x_2 \oplus x_3 \oplus 1$. Поэтому в базисе B функции $x_2 \oplus x_3$ и $x_2 \oplus x_3 \oplus 1$ можно реализовать схемами S_1 и S_2 соответственно, каждая из которых содержит не более трёх элементов. Пусть, как и раньше, $P(S_\oplus) = \max\{P(S_1), P(S_2)\}$. Ясно, что $P(S_\oplus) \leqslant 3\varepsilon$. Тогда, применяя лемму 1, построим схему S_g, реализующую функцию $g \in G_1$, такую, что $P(S_g) \leqslant 9\varepsilon$, а $v^1, v^0 \leqslant 3\varepsilon + 2 \cdot 3\varepsilon \cdot 3\varepsilon + (3\varepsilon)^2 = 3\varepsilon + 27\varepsilon^2$. По теореме 2 при $\varepsilon \leqslant 1/960$ любую булеву функцию f можно реализовать схемой A такой, что $P(A) \leqslant 5{,}2\varepsilon$. Применяя теорему 1, по схеме A построим реализующую функцию f схему S такую, что

$$P(S) \leqslant 3\varepsilon + 27\varepsilon^2 + 3 \cdot 5{,}2\varepsilon \cdot 9\varepsilon + 3(5{,}2\varepsilon)^2 \leqslant 3\varepsilon + 249\varepsilon^2.$$

(b) Пусть базис B содержит константу 1. Нетрудно проверить, что $\varphi(0, x_2, x_3) = x_2 \oplus x_3$ и $\varphi(0, 1, \varphi(0, x_2, x_3)) = x_2 \oplus x_3 \oplus 1$. Тогда $P(S_\oplus) \leqslant 4\varepsilon$.

Применяя лемму 1, построим схему S_g, реализующую функцию $g \in G_1$ такую, что $P(S_g) \leqslant 11\varepsilon$, а

$$v^1, v^0 \leqslant 3\varepsilon + 2 \cdot 3\varepsilon \cdot 4\varepsilon + (4\varepsilon)^2 = 3\varepsilon + 40\varepsilon^2.$$

По теореме 2 при $\varepsilon \leqslant 1/960$ любую булеву функцию f можно реализовать схемой A такой, что $P(A) \leqslant 5{,}2\varepsilon$. Применяя теорему 1, по схеме A построим реализующую функцию f схему S такую, что

$$P(S) \leqslant 3\varepsilon + 40\varepsilon^2 + 3 \cdot 5{,}2\varepsilon \cdot 11\varepsilon + 3(5{,}2\varepsilon)^2 \leqslant 3\varepsilon + 293\varepsilon^2.$$

Теорема 9 доказана.

Теорема 10. *Пусть полный конечный базис* $B \subset (\Psi^* \cup \{\overline{x}, 0, 1\}) \backslash H$ *удовлетворяет хотя бы одному из следующих условий*:

(i) *B содержит функцию, конгруэнтную* $\varphi = x_1 \vee x_2^{\sigma_2} x_3^{\sigma_3}$, $\sigma_2, \sigma_3 \in \{0, 1\}$;

(ii) *B содержит константу* 0 *и функцию, конгруэнтную* $\varphi = x_1 \vee (x_2 \oplus x_3 \oplus \sigma_3)$, $\sigma_3 \in \{0, 1\}$;

(iii) *B содержит функцию, конгруэнтную* $\varphi = \overline{x}_1 \vee (x_2 \oplus x_3 \oplus 1)$.

Тогда произвольную булеву функцию f в базисе B можно реализовать схемой S такой, что $P(S) \leqslant 3\varepsilon + 293\varepsilon^2$ *при любом* $\varepsilon \in (0, 1/960]$.

Доказательство. Утверждение теоремы следует из теорем 9 и 3.

2. Нижние оценки ненадёжности схем

Пусть $K(n)$ — множество булевых функций $f(x_1, x_2, \ldots, x_n)$, не представимых в виде $\left(x_i^a \& h(\widetilde{x})\right)^b$ или $((x_i \oplus x_j)^a \cdot h(\widetilde{x}))^b$, где $h(\widetilde{x})$ — произвольная функция, $i \neq j,\ i, j \in \{1, 2, \ldots, n\},\ a, b \in \{0, 1\}$.

Поскольку $|P_2(n) \backslash K(n)| \leqslant 2 \cdot (2n \cdot 2^{2^{n-1}} + (n^2 - n) \cdot (2^{2^{n-2}})^2)$, имеем $|K(n)| \geqslant 2^{2^n} - 2^{2^{n-1}+1} \cdot (n^2 + n)$.

Утверждение 1 [8]. *Пусть функция* $f(x, y) = \min\left\{\frac{x}{x+y}, \frac{y}{x+y}\right\}$ *задана в прямоугольнике* $D = \{(x, y) \mid a \leqslant x \leqslant b,\ a \leqslant y \leqslant b,\ 0 < a < b\}$. *Тогда* $\max\limits_D f(x, y) = \frac{1}{2}$, $\min\limits_D f(x, y) = \frac{a}{a+b}$.

Лемма 4 [7]. *Пусть* $\varepsilon \in (0, 1/960]$, $f \in K(n)$ — *булева функция, а* S — *реализующая* f *схема такая, что* $P(S) \leqslant 5{,}2\varepsilon$. *Если в схеме* S *можно выделить связную подсхему* A, *функционирующую с ненадёжностью* $P(A) \leqslant 4\varepsilon(1 - \varepsilon)^3$, *состоящую хотя бы из четырёх элементов, имеющую один вход и содержащую выход схемы, то схема* S *не является bc-схемой.*

Доказательство. Пусть схема S является bc-схемой и A — связная подсхема схемы S, состоящая хотя бы из одного элемента, имеющая один вход и содержащая выход схемы S. Нетрудно проверить, что $P(A) \geqslant \varepsilon$. По условию $P(A) \leqslant 4\varepsilon(1 - \varepsilon)^3$. Следовательно,

$$\varepsilon \leqslant P(A) \leqslant 4\varepsilon(1 - \varepsilon)^3.$$

Тогда вероятности ошибок p_0 и p_1 для схемы A по определению ненадёжности также удовлетворяют этому неравенству. По утверждению 1 имеем

$$\frac{1}{5} < \frac{\varepsilon}{\varepsilon + 4\varepsilon(1 - \varepsilon)^3} \leqslant \min\left\{\frac{p_0}{p_0 + p_1}, \frac{p_1}{p_0 + p_1}\right\}.$$

С другой стороны, по теореме 5

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

Таким образом, $\frac{1}{5} < \min\left\{\frac{p_0}{p_0+p_1}, \frac{p_1}{p_0+p_1}\right\} \leqslant P(S) \leqslant 5{,}2\varepsilon$, т. е. $\frac{1}{5} < 5{,}2\varepsilon$, что неверно при $\varepsilon \in (0, 1/960]$. Лемма 4 доказана.

Теорема 11 [7]. *Пусть* B — *полный базис такой, что либо* $B \subset (\Theta \cup \Theta^* \cup \{\overline{x}_1, 0, 1\})$, *либо* $B \subset (\Psi \cup \{\overline{x}_1, 0, 1\})$, *либо* $B \subset (\Psi^* \cup \{\overline{x}_1, 0, 1\})$. *Если* $f(\widetilde{x}) \in K(n)$, *а* S — *любая схема, реализующая функцию* f, *то* $P(S) \geqslant 3\varepsilon(1 - \varepsilon)^3$ *при любом* $\varepsilon \in (0, 1/960]$.

Замечание 1. Из результатов работ [3, 4, 6, 7] известно, что во всех базисах $B \subseteq B_3$, не удовлетворяющих условиям теоремы 11, ненадёжность асимптотически оптимальных по надёжности схем для всех функций асимптотически равна ε или 2ε при $\varepsilon \to 0$.

Введём обозначения:

Ω — множество функций, зависящих от переменных x_1, x_2, x_3, конгруэнтных функциям x_1x_2, $\overline{x}_1x_2$, $x_1x_2x_3$, $\overline{x}_1x_2x_3$, $\overline{x}_1\overline{x}_2x_3$;

Ω^* — множество функций, двойственных функциям множества Ω;

Ω_1 — множество, состоящее из функций множества Ω и функций, конгруэнтных функциям $x_1(x_2 \oplus x_3 \oplus \sigma)$, где $\sigma \in \{0, 1\}$;

Ω_1^* — множество функций, двойственных функциям множества Ω_1.

Набор $\widetilde{a} = (a_1, a_2, \ldots, a_n)$ называется *нулевым* (*единичным*) для функции $f(x_1, x_2, \ldots, x_n)$, если $f(a_1, a_2, \ldots, a_n)$ равно нулю (единице).

Теорема 12. *Пусть B — полный базис такой, что либо $B \subset (\Omega \cup \{\overline{x}_1, 0, 1\})$, либо $B \subset (\Omega^* \cup \{\overline{x}_1, 0, 1\})$, либо $B \subset (\Omega_1 \cup \{\overline{x}_1, 0\})$, либо $B \subset (\Omega_1^* \cup \{\overline{x}_1, 1\})$. Если $f(\widetilde{x}) \in K(n)$, S — любая схема, реализующая функцию f, то $P(S) \geqslant 4\varepsilon(1-\varepsilon)^3$ при любом $\varepsilon \in (0, 1/960]$.*

Доказательство. Пусть B — любой из базисов, удовлетворяющих условию теоремы, а S — произвольная схема, реализующая функцию $f(\widetilde{x}) \in K(n)$. Без ограничения общности схему S можно считать bc-схемой.

Пусть A — связная подсхема схемы S, состоящая хотя бы из одного элемента и содержащая выход схемы. Обозначим через $p_{11}, \ldots, p_{1k}$ всевозможные различные вероятности ошибок на выходе схемы A при нулевых входных наборах $\widetilde{b}$ схемы A. Аналогично, пусть $p_{01}, \ldots, p_{0m}$ — всевозможные различные вероятности ошибок на выходе схемы A при единичных входных наборах $\widetilde{b}$ схемы A. Полагаем $p^1 = \min\{p_{11}, \ldots, p_{1k}\}$, $p^0 = \min\{p_{01}, \ldots, p_{0m}\}$.

Оценим ненадёжность схемы S.

(i) Пусть подсхема A имеет один вход, тогда A реализует тождественную функцию или инверсию (так как $f(\widetilde{x}) \in K(n)$ и $0, 1 \notin K(n)$). Возможны два варианта:

(a) $P(A) > 4\varepsilon(1-\varepsilon)^3$, тогда этому неравенству удовлетворяет хотя бы одно из чисел p^0 или p^1, и по следствию 1 получаем $P(S) > 4\varepsilon(1-\varepsilon)^3$;

(b) $P(A) \leqslant 4\varepsilon(1-\varepsilon)^3$, что противоречит лемме 4.

(ii) Пусть в схеме S нельзя выделить подсхему A, имеющую ровно один вход и содержащую выход схемы. Тогда выделим связную подсхему C схемы S из четырёх элементов E_1, E_2, E_3, E_4, содержащую выход

схемы S (это можно сделать, так как $f(\widetilde{x}) \in K(n)$). Обозначим через E_1 выходной элемент схемы C.

(ii.1) Рассмотрим базисы $B \subset (\Omega \cup \{\overline{x}_1, 0, 1\})$. Возможны следующие варианты.

(ii.1.1) Пусть элементу E_1 приписана функция e_1, конгруэнтная функции $x_1^{\sigma_1} x_2$ ($\sigma_1 \in \{0,1\}$). Тогда в схеме S найдутся различные элементы E_2 и E_3 такие, что их выходы соединены со входами элемента E_1 (так как схема S реализует функцию $f \in K(n)$, ни один вход элемента E_1 не может быть соединён с полюсом схемы S). Не ограничивая общности, в этом случае будем считать, что выход элемента E_2 соединён с первым входом элемента E_1, а выход элемента E_3 — со вторым входом элемента E_1. Заметим, что элементам E_2 и E_3 не может быть приписана константа 0 или 1 (иначе либо $f \notin K(n)$, либо случай рассмотрен в (i)). Заметим, что ни один вход элемента E_3 не может быть соединён с полюсом схемы S, поэтому в схеме S найдётся элемент E_4, выход которого соединён с одним из входов элемента E_3. Если при поступлении единичного набора $\widetilde{\alpha}$ на вход схемы C, состоящей из элементов E_1, E_2, E_3, E_4, ошибается только один элемент E_1, то на выходе всей схемы вместо 1 появится 0. Если при поступлении единичного набора $\widetilde{\alpha}$ на вход схемы C ошибается ровно один из элементов E_2, E_3 или E_4, то на вход элемента E_1 поступит набор, отличный от единственного единичного набора $(\sigma_1, 1)$ функции e_1, значит, на выходе всей схемы вместо 1 появится 0. Поэтому $p^0 \geqslant 4\varepsilon(1-\varepsilon)^3$. Тогда по следствию 1 $P(S) \geqslant 4\varepsilon(1-\varepsilon)^3$.

(ii.1.2) Пусть элементу E_1 приписана функция e_1, конгруэнтная функции $x_1^{\sigma_1} x_2^{\sigma_2}\ x_3$ ($\sigma_1, \sigma_2 \in \{0,1\}$) и некоторые два входа элемента E_1 отождествлены. Тогда либо вся схема S реализует константу 0 (что противоречит условию $f \in K(n)$), либо элемент E_1 реализует функцию $x_1^{\sigma_1} x_2$, которая рассмотрена в (ii.1.1). Следовательно, утверждение теоремы верно.

(ii.1.3) Пусть элементу E_1 приписана функция e_1, конгруэнтная функции $x_1^{\sigma_1} x_2^{\sigma_2} x_3$ ($\sigma_1, \sigma_2 \in \{0,1\}$), и никакие входы элемента E_1 не отождествлены. Тогда в схеме S найдутся такие три различные элемента E_2, E_3 и E_4, что их выходы соединены с входами элемента E_1 (так как схема S реализует функцию $f \in K(n)$, ни один вход элемента E_1 не может быть соединён с полюсом схемы S). Не ограничивая общности, в этом случае будем считать, что выход элемента E_i соединён с $(i-1)$-м входом элемента E_1 ($i = 2, 3, 4$). Заметим, что элементам E_2, E_3 и E_4 не может быть приписана константа 0 или 1 (иначе либо $f \notin K(n)$, либо имеем один из вариантов, рассмотренных выше). Если при поступле-

нии единичного набора $\widetilde{\alpha}$ на вход схемы C из элементов E_1, E_2, E_3, E_4 ошибается только один элемент E_1, то на выходе всей схемы вместо 1 появится 0. Если при поступлении единичного набора $\widetilde{\alpha}$ на вход схемы C ошибается ровно один из элементов E_2, E_3 или E_4, то на вход элемента E_1 поступит набор, отличный от единственного единичного набора $(\sigma_1, \sigma_2, 1)$ функции e_1, значит, на выходе всей схемы вместо 1 появится 0. Поэтому $p^0 \geqslant 4\varepsilon(1-\varepsilon)^3$. Тогда по следствию 1 $P(S) \geqslant 4\varepsilon(1-\varepsilon)^3$.

Таким образом, в базисах $B \subset (\Omega \cup \{\overline{x}_1, 0, 1\})$ утверждение теоремы верно.

(ii.2) Рассмотрим базисы $B \subset (\Omega_1 \cup \{\overline{x}_1, 0\})$. Возможны следующие варианты.

(ii.2.1) Пусть элементу E_1 приписана функция e_1, конгруэнтная одной из функций $x_1^{\sigma_1}x_2$, $x_1^{\sigma_1}x_2^{\sigma_2}x_3$ $(\sigma_1, \sigma_2 \in \{0,1\})$. Тогда, повторяя рассуждения (ii.1), убеждаемся в верности утверждения теоремы.

(ii.2.2) Пусть элементу E_1 приписана функция e_1, конгруэнтная функции $x_1(x_2 \oplus x_3 \oplus \sigma_3)$ $(\sigma_3 \in \{0,1\})$ и некоторые входы элемента E_1 отождествлены. Тогда либо вся схема S реализует константу 0 (что противоречит условию $f \in K(n)$), либо тождественную функцию (см. (i)), либо элемент E_1 реализует функцию, конгруэнтную функции $x_1^{\sigma_1}x_2$ (этот случай рассмотрен в (ii.1.1)). Во всех случаях утверждение теоремы верно.

(ii.2.3) Пусть элементу E_1 приписана функция e_1, конгруэнтная функции $x_1(x_2 \oplus x_3 \oplus \sigma_3)$ $(\sigma_3 \in \{0,1\})$ и никакие входы элемента E_1 не отождествлены. Тогда в схеме S найдутся два различных элемента E_2, E_3 такие, что выход элемента E_2 соединён с первым входом элемента E_1 и выход элемента E_3 соединён с вторым или третьим входом элемента E_1 (так как схема S реализует функцию $f \in K(n)$). Не ограничивая общности, в этом случае будем считать, что выход элемента E_i соединён с $(i-1)$-м входом элемента E_1 $(i = 2, 3)$. Заметим, что элементам E_2 и E_3 не может быть приписана константа 0 (иначе либо $f \notin K(n)$, либо это случай (ii.1.1)).

Пусть элементу E_2 приписана функция $e_2 \in \Omega_1$ (случай $e_2 = \overline{x}$ противоречит условию $f \in K(n)$). Тогда первый вход элемента E_2 не может быть соединён с полюсом схемы S $(f \notin K(n))$, стало быть, он соединён с выходом некоторого элемента. Возможны следующие варианты.

(ii.2.3a) Первый вход элемента E_2 соединён с выходом элемента E_3. Тогда в схеме S найдётся элемент E_4, выход которого соединён с первым входом элемента E_3.

(ii.2.b) Первый вход элемента E_2 не соединён с выходом элемента E_3.

Тогда в схеме S найдётся элемент E_4, выход которого соединён с первым входом элемента E_2.

Если при поступлении единичного набора $\widetilde{\alpha}$ на вход схемы C из элементов E_1, E_2, E_3, E_4 ошибается только элемент E_1, то на выходе всей схемы вместо 1 появится 0. Если при поступлении единичного набора $\widetilde{\alpha}$ на вход схемы C ошибается ровно один из элементов E_2, E_3 или E_4, то на вход элемента E_1 поступит набор, отличный от единичных наборов $(1, 0, \sigma_3 \oplus 1)$ и $(1, 1, \sigma_3)$ функции e_1, значит, на выходе всей схемы вместо 1 появится 0. Поэтому $p^0 \geqslant 4\varepsilon(1-\varepsilon)^3$. Тогда по следствию 1 верно неравенство $P(S) \geqslant 4\varepsilon(1-\varepsilon)^3$.

Таким образом, в базисах $B \subset (\Omega_1 \cup \{\overline{x}_1, 0\})$ утверждение теоремы верно.

(ii.3) Если $B \subset (\Omega^* \cup \{\overline{x}_1, 0, 1\})$ или $B \subset (\Omega_1^* \cup \{\overline{x}_1, 1\})$, то по теореме 3 и в силу предыдущих пунктов утверждение теоремы верно. Теорема 12 доказана.

3. Выводы

Из теоремы 11 следует, что если полный базис B удовлетворяет условиям хотя бы одной из теорем 6–10, то в B почти все булевы функции можно реализовать асимптотически оптимальными схемами, функционирующими с ненадёжностью 3ε при $\varepsilon \to 0$.

Из теоремы 12 и замечания 1 следует, что других базисов $B \subset B_3$, в которых почти все булевы функции можно реализовать асимптотически оптимальными схемами, функционирующими с ненадёжностью 3ε при $\varepsilon \to 0$, нет.

ЛИТЕРАТУРА

1. **Алёхина М. А.** Синтез асимптотически оптимальных по надёжности схем из ненадёжных элементов. — Пенза: ИИЦ ПГУ, 2006. — 156 с.
2. **Алёхина М. А.** О надёжности и сложности схем в базисе $\{x|y\}$ при инверсных неисправностях элементов. // Дискрет. анализ и исслед. операций. Сер. 1. — 2005. — Том 12, № 2. — С. 3–11.
3. **Алёхина М. А., Васин А. В.** О надёжности схем в базисах, содержащих функции не более чем трёх переменных // Уч. зап. Казан. гос. ун-та. Сер. Физ-мат. науки. — 2009. — Т. 151, № 2. — С. 25–35.
4. **Алёхина М. А., Васин А. В.** Достаточные условия реализации булевых функций асимптотически оптимальными схемами с ненадёжностью 2ε // Изв. вузов. Математика. — 2010. — № 5. — С. 79–82.

5. **Алёхина М. А., Пичугина П. Г.** О надёжности двойственных схем в полном конечном базисе // Мат. XVIII междунар. шк.–семинара «Синтез и сложность управляющих систем» (г. Пенза, 28 сентября–3 октября 2009 г.). — М.: Изд-во мех.-мат. фак-та МГУ, 2009. — С. 10–13.
6. **Васин А. В.** О функциях специального вида // Тр. VIII междунар. конф. «Дискретные модели в теории управляющих систем» (Лесной городок, Моск. обл., 6–9 апреля 2009 г.). — М.: МАКС Пресс, 2009. — С. 43–47.
7. **Васин А. В.** Необходимые и достаточные условия реализации булевых функций асимптотически оптимальными схемами с ненадёжностью 2ε // Мат. X междунар. семинара «Дискретная математика и её приложения» (Москва, 1–6 февраля 2010 г.). — М.: Изд-во мех.-мат. фак-та МГУ, 2010. — С. 94–97.
8. **Васин А. В.** Об асимптотически оптимальных схемах в базисе $\{\&, \neg\}$ при инверсных неисправностях на выходах элементов // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 6. — С. 12–22.
9. **Нейман Дж.** Автоматы. — М.: Изд-во иностр. лит., 1956. — С. 68–139.

Васин Алексей Валерьевич,
e-mail: alvarvasin@mail.ru

Статья поступила
12 апреля 2010 г.

Переработанный вариант —
17 января 2013 г.