Известия вузов. Математика *http://www.ksu.ru/journals/izv_vuz/*
2012, № 2, с. 13–22 *Гос. номер статьи по НТЦ "Информрегистр" 0421200123\0015*

М.А. АЛЕХИНА, С.М. ГРАБОВСКАЯ

О НАДЕЖНОСТИ НЕВЕТВЯЩИХСЯ ПРОГРАММ В ПРОИЗВОЛЬНОМ ПОЛНОМ КОНЕЧНОМ БАЗИСЕ

Аннотация. Рассматривается реализация булевых функций неветвящимися программами с условной остановкой в произвольном полном конечном базисе. Предполагается, что операторы условной остановки абсолютно надежны, а все вычислительные операторы базиса независимо друг от друга с вероятностью ε из интервала $(0, 1/2)$ подвержены инверсным неисправностям на выходах. Доказано, что любую булеву функцию можно реализовать программой с ненадежностью $\varepsilon + 81\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Ключевые слова: булевы функции, неветвящиеся программы, оператор условной остановки, синтез, надежность.

УДК: 519.718

Abstract. We consider the realization of Boolean functions by nonbranching programs with conditional stop-operators in an arbitrary complete finite basis. We assume that conditional stop-operators are absolutely reliable, while all functional operators are prone to output inverse failures independently of each other with probability ε from the interval $(0, 1/2)$. We prove that any Boolean function is realizable by a nonbranching program with unreliability $\varepsilon + 81\varepsilon^2$ for all $\varepsilon \in (0, 1/960]$.

Keywords: boolean functions, nonbranching programs, conditional stop-operator, synthesis, reliability.

1. Необходимые определения и обозначения

Рассматривается реализация булевых функций неветвящимися программами с операторами условной остановки [1], [2] в полном конечном базисе B. Программы с операторами условной остановки характеризуются наличием управляющих команд – команд условной остановки, дающих возможность досрочного прекращения работы при выполнении определенного условия. Сформулируем необходимые понятия и определения [1], [2].

Пусть $X = \{x_1, \dots, x_n\}$ — множество независимых булевых переменных, $\widetilde{x} = (x_1, \dots, x_n)$ — набор независимых переменных, $n \in N$. Введем множество переменных $Y = \{y_1, \dots, y_l\}$, которое назовем множеством внутренних переменных, $l \in N$. Кроме того, через z обозначим выходную переменную.

Пусть далее $a \in Y \cup \{z\}$, $b_1, \dots, b_d \in X \cup Y \cup \{z\}$ $(d \in \{1, \dots, n\})$, h — булева функция из базиса B, зависящая не более чем от d переменных. Вычислительной командой назовем

Поступила 02.02.2011

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 11-01-00212-а).

выражение $p:\ a = h(b_1, \dots, b_d)$. Переменную a назовем выходом вычислительной команды, переменные $b_1, \dots, b_d$ — входами этой команды.

Пусть теперь $a \in X \cup Y \cup \{z\}$. Командой остановки назовем выражение p : $\mathrm{Stop}(a)$. Переменную a назовем входом команды остановки p.

Последовательность $\mathrm{Pr} = p_1 \dots p_j \dots p_L$, состоящая из вычислительных команд и команд остановки, называется неветвящейся программой с условной остановкой, если при любом $j \in \{1, \dots, L\}$ каждый вход команды p_j есть либо независимая переменная, либо выход некоторой вычислительной команды.

Неветвящаяся программа работает в дискретные моменты времени $t = 0, 1, 2, \dots$, не изменяет значения независимых переменных и изменяет значения внутренних переменных y_i $(i \in \{1, \dots, l\})$ и значение выходной переменной z. Значения $y_i(\widetilde{x}; t)$ внутренних переменных y_i (или значение $z(\widetilde{x}; t)$ выходной переменной z) программы Pr в произвольный момент времени t на наборе $\widetilde{x}$ независимых переменных $x_1, \dots, x_n$ определим индуктивно следующим образом:

- в начальный момент времени $t = 0$ значения всех внутренних (и выходной) переменных считаем неопределенными;
- если команда p_t не изменяет значения внутренней переменной y_i (или выходной переменной z), то положим $y_i(\widetilde{x};\ t) = y_i(\widetilde{x}; t-1)$ (или $z(\widetilde{x}; t) = z(\widetilde{x}; t-1)$);
- если команда p_t изменяет значения внутренней переменной y_i (или выходной переменной z) и значения 1-го, …, d-го входов команды p_t в момент времени $t-1$ равны соответственно $b_1(\widetilde{x}; t-1), \dots, b_d(\widetilde{x}; t-1)$, то полагаем

$$y_i(\widetilde{x}; t) = h_t(b_1(\widetilde{x}; t-1), \dots, b_d(\widetilde{x}; t-1))\ (\text{или} z(\widetilde{x}; t) = h_t(b_1(\widetilde{x}; t-1), \dots, b_d(\widetilde{x}; t-1))).$$

Значением команды p_t программы Pr на наборе $\widetilde{x}$ независимых переменных $x_1, x_2, \dots, x_n$ назовем значение ее выхода в момент времени t и обозначим $p_t(\widetilde{x})$. Пусть $p_{t_1}, \dots, p_{t_r}$ — все команды остановки из Pr, причем $t_1 < \dots < t_r$, т.е. r — число команд остановки. Тогда через s_j будем обозначать j-ю команду остановки программы Pr (т. е. $s_j \equiv p_{t_j}$), а через q_j — аргумент команды остановки s_j.

Будем говорить, что 1-я команда остановки s_1 прекращает вычисления программы Pr на наборе $\widetilde{x}$, если $q_1(\widetilde{x}) = 1$; k-я команда остановки s_k $(k \in \{2, \dots, r\})$ прекращает вычисления программы Pr на наборе $\widetilde{x}$, если $q_1(\widetilde{x}) = \dots = q_{k-1}(\widetilde{x}) = 0,\ q_k(\widetilde{x}) = 1$.

Результат действия программы Pr на наборе $\widetilde{x}$ обозначим через $\mathrm{Pr}(\widetilde{x})$ и определим следующим образом:

$$\mathrm{Pr}(\widetilde{x}) = \begin{cases} z(\widetilde{x}; t_1), & \text{если } q_1(\widetilde{x}) = 1; \\ z(\widetilde{x}; t_k), & \text{если } q_1(\widetilde{x}) = \dots = q_{k-1}(\widetilde{x}) = 0,\ q_k(\widetilde{x}) = 1 \quad (k = 2, \dots, r); \\ z(\widetilde{x}; L), & \text{если } q_1(\widetilde{x}) = \dots = q_r(\widetilde{x}) = 0, \end{cases}$$

т. е. $\mathrm{Pr}(\widetilde{x})$ равно значению выходной переменной z в момент остановки программы. Легко видеть, что

$$\mathrm{Pr}(\widetilde{x}) = q_1(\widetilde{x})z(\widetilde{x}; t_1) \vee \overline{q}_1(\widetilde{x})q_2(\widetilde{x})z(\widetilde{x}; t_2) \vee \dots \vee \overline{q}_1(\widetilde{x})\overline{q}_2(\widetilde{x}) \cdots \overline{q}_{k-1}(\widetilde{x})q_k(\widetilde{x})z(\widetilde{x}; t_k) \vee \cdots$$
$$\cdots \vee \overline{q}_1(\widetilde{x})\overline{q}_2(\widetilde{x}) \cdots \overline{q}_{r-1}(\widetilde{x})q_r(\widetilde{x})z(\widetilde{x}; t_r) \vee \overline{q}_1(\widetilde{x})\overline{q}_2(\widetilde{x}) \cdots \overline{q}_r(\widetilde{x})z(\widetilde{x}; L). \quad (1)$$

Иногда формулу (1) удобнее использовать в преобразованном виде

$$\mathrm{Pr}(\widetilde{x}) = q_1(\widetilde{x})z(\widetilde{x}; t_1) \vee \overline{q}_1(\widetilde{x})(q_2(\widetilde{x})z(\widetilde{x}; t_2) \vee \overline{q}_2(\widetilde{x})(\cdots$$
$$\cdots (q_{k-1}(\widetilde{x})z(\widetilde{x}; t_{k-1}) \vee \overline{q}_{k-1}(\widetilde{x})(\cdots \vee \overline{q}_{r-1}(\widetilde{x})(q_r(\widetilde{x})z(\widetilde{x}; t_r) \vee \overline{q}_r(\widetilde{x})z(\widetilde{x}; L)) \cdots)) \cdots)). \quad (2)$$

Программа Pr вычисляет n-местную булеву функцию f, если $\mathrm{Pr}(\widetilde{x}) = f(\widetilde{x})$ для любого $\widetilde{x}$ из $\{0,1\}^n$. Всюду далее будем считать, что все операторы условной остановки абсолютно надежны (и, значит, срабатывают, если на вход поступает единица), а все вычислительные операторы базиса B независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах. Инверсные неисправности на выходах вычислительных операторов характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему функцию φ, а в неисправном — функцию $\overline{\varphi}$.

Считаем, что программа с ненадежными вычислительными операторами реализует булеву функцию $f(\widetilde{x})$, если при отсутствии неисправностей в ней на каждом входном наборе $\widetilde{a}$ значение выходной переменной z равно $f(\widetilde{a})$.

Нетрудно видеть, что схемы из функциональных элементов являются частным случаем неветвящихся программ с оператором условной остановки, точнее, схему из функциональных элементов можно считать программой, в которой нет ни одного оператора условной остановки.

Ненадежностью $N_\varepsilon(\mathrm{Pr})$ программы Pr назовем максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах. Надежность программы Pr равна $1 - N_\varepsilon(\mathrm{Pr})$.

Обозначим $N_\varepsilon(f) = \inf N_\varepsilon(\mathrm{Pr})$, где инфимум берется по всем программам Pr, реализующим булеву функцию $f(\widetilde{x})$.

Программа A, реализующая функцию f, называется асимптотически оптимальной по надежности, если $N_\varepsilon(A) \sim N_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon\to 0} \frac{N_\varepsilon(f)}{N_\varepsilon(A)} = 1$.

2. Известные результаты, постановка задачи

Теорема 1 ([3]). *В произвольном полном конечном базисе любую булеву функцию f можно реализовать схемой S, ненадежность которой $N_\varepsilon(S) \leqslant 5\varepsilon + 182\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

Константа 5 в оценке ненадежности из теоремы 1 в некоторых базисах, например, $B = \{x_1\&x_2, \overline{x}_1\}$, не может быть понижена [4].

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

Пусть B_3 — множество всех булевых функций, зависящих от трех переменных x_1, x_2, x_3, а $X \subseteq B_3$. Обозначим через $\mathrm{Congr}(X)$ множество всех функций, зависящих от переменных x_1, x_2, x_3, каждая из которых конгруэнтна некоторой функции множества X. Например, если $X = \{x_1,\ x_1\&x_2,\ 1\}$, то $\mathrm{Congr}(X) = \{x_1,\ x_2,\ x_3,\ x_1\&x_2,\ x_1\&x_3,\ x_2\&x_3,\ 1\}$.

Обозначим $G = G_1 \cup G_2 \cup G_3$, где $G_1 = \{x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$; $G_2 = \mathrm{Congr}\{x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$; $G_3 = \mathrm{Congr}\{x_1^{\sigma_1}x_2^{\overline{\sigma}_2} \vee x_2^{\sigma_2}x_3^{\sigma_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$.

Теорема 2 ([5], с. 34). (1) *Если в полном конечном базисе содержится функция $\varphi \in G$, то в этом базисе любую булеву функцию можно реализовать схемой, ненадежность которой не больше $\varepsilon + 200\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

(2) *Если в полном конечном базисе содержится функция $\varphi \in G_1$, то в этом базисе любую булеву функцию можно реализовать схемой, ненадежность которой не больше $\varepsilon + 8\varepsilon^2$ при всех $\varepsilon \in (0,\ 1/960]$.*

Теорема 3 ([5], с. 36). *Пусть B — произвольный полный конечный базис, f — любая функция, для реализации которой требуется не менее одного функционального элемента. Тогда для любой схемы S, реализующей f, в базисе B верно неравенство $N_\varepsilon(S) \geqslant \varepsilon$ при всех $\varepsilon \in (0,\ 1/2)$.*

Из теорем 2 и 3 следует, что если полный конечный базис содержит функцию $\varphi \in G$, то почти все булевы функции в этом базисе можно реализовать асимптотически оптимальными по надежности схемами, ненадежность которых асимптотически равна ε при $\varepsilon \to 0$.

Обозначим через $K_2(n)$ множество всех булевых функций $f(x_1, \ldots, x_n)$ $(n \geqslant 3)$, не представимых в виде $(x_i^a \& h(\widetilde{x}))^b$ или $(x_i^a \& x_j^b \vee x_i^{\overline{a}} \& x_j^{\overline{b}} \& h(\widetilde{x}))^c$, где $h(\widetilde{x})$ — произвольная функция, $i, j \in \{1, \ldots, n\}$, $a, b, c \in \{0, 1\}$. Доказано ([3]; [5], с. 57), что $|K_2(n)| \geqslant 2^{2^n} - 4(n2^{2^{n-1}} + (n^2 - n)2^{2^{n-2}})$. Пусть $K_2 = \bigcup\limits_{n=3}^{\infty} K_2(n)$.

Теорема 4 ([5], с. 57). *Пусть полный базис $B \subseteq B_3 \setminus G$, $f \in K_2$ и S — любая схема в базисе B, реализующая функцию f. Тогда $N_\varepsilon(S) \geqslant 2\varepsilon - 2\varepsilon^2$ при любом $\varepsilon \in (0, 1/4]$.*

Из теорем 2, 3 и 4 следует, что в полном базисе $B \subseteq B_3$ почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью ε при $\varepsilon \to 0$, тогда и только тогда, когда $B \cap G \neq \emptyset$.

Известно [5], что в различных полных базисах $B \subseteq B_3 \setminus G$ почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами из функциональных элементов с ненадежностью, асимптотически равной $k_B\varepsilon$ при $\varepsilon \to 0$. Константа k_B зависит от базиса B и $k_B \in \{2, 3, 4, 5\}$.

Иначе обстоит дело с ненадежностью неветвящихся программ. Далее будет доказано, что в любом полном конечном базисе произвольную булеву функцию можно реализовать неветвящейся программой с ненадежностью не больше $\varepsilon + 81\varepsilon^2$ при всех $\varepsilon \in (0,\ 1/960]$.

Булевы функции $x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus c_1x_1 \oplus c_2x_2 \oplus c_3x_3 \oplus c_0$ $(c_i \in \{0, 1\},\ i \in \{0, 1, 2, 3\})$ будем называть особенными [6].

Лемма 1 ([6]). *Из всякой нелинейной неособенной функции от трех или более переменных отождествлением переменных можно получить либо нелинейную функцию от двух переменных, либо особенную функцию.*

Другими словами, из всякой нелинейной функции подстановкой (отождествлением и/или переименованием [7]) переменных можно получить либо некоторую нелинейную функцию двух переменных $\phi(x_1, x_2) = x_1x_2 \oplus c_1x_1 \oplus c_2x_2 \oplus c_0$, либо некоторую особенную функцию $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus c_1x_1 \oplus c_2x_2 \oplus c_3x_3 \oplus c_0$, где $c_0, c_1, c_2, c_3 \in \{0, 1\}$.

Для нелинейной функции двух переменных справедлива

Теорема 5 ([8], [9]). *В полном конечном базисе, содержащем нелинейную функцию двух переменных, любую функцию f можно реализовать такой программой Pr_f, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\varepsilon(\mathrm{Pr}_f) \leqslant \varepsilon + 81\varepsilon^2$.*

Поэтому далее будем рассматривать только те полные конечные базисы, в которых из нелинейной функции подстановкой переменных можно получить некоторую особенную функцию. Для базисов, содержащих особенную функцию, справедлива теорема 6.

3. Основные результаты

Теорема 6. *В полном конечном базисе, содержащем особенную функцию, любую функцию f можно реализовать такой программой Pr_f, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\varepsilon(\mathrm{Pr}_f) \leqslant \varepsilon + 81\varepsilon^2$.*

Из леммы 1 и теорем 5, 6 следует основное утверждение данной работы.

Теорема 7. *В произвольном полном конечном базисе любую функцию f можно реализовать такой программой Pr_f, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство*

$$N_\varepsilon(\mathrm{Pr}_f) \leqslant \varepsilon + 81\varepsilon^2.$$

Доказательству теоремы 6 предпошлем леммы 2–7.

Лемма 2. *Если полный конечный базис содержит функцию $\varphi_1(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$, то в этом базисе функцию $g(x_1, x_2, x_3) = \overline{x}_1x_2 \vee x_2x_3 \vee \overline{x}_1x_3 \in G_1$ можно реализовать неветвящейся программой Pr_g^1 с ненадежностью $N_\varepsilon(\mathrm{Pr}_g^1) \leqslant \varepsilon$:*

$$\begin{array}{l}
\mathrm{Pr}_g^1(x_1, x_2, x_3):\\
z = \varphi_1(x_1, x_2, x_3)\\
\mathrm{stop}(x_1)\\
z = x_2\\
\mathrm{stop}(x_2)\\
z = x_3.
\end{array}$$

Доказательство. Пусть B — полный конечный базис, $\varphi_1(x_1, x_2, x_3) \in B$. Нетрудно проверить, что $\varphi_1(x_1, x_2, x_3) = x_1x_2x_3 \vee \overline{x}_1\overline{x}_2\overline{x}_3$. По формуле (2) найдем функцию, которую вычисляет программа Pr_g^1:

$$\mathrm{Pr}_g^1(x_1, x_2, x_3) = \varphi_1(x_1, x_2, x_3)x_1 \vee \overline{x}_1(x_2 \vee \overline{x}_2x_3) = \varphi_1(x_1,\ x_2,\ x_3)x_1 \vee \overline{x}_1(x_2 \vee x_3) =$$
$$= x_1x_2x_3 \vee \overline{x}_1x_2 \vee \overline{x}_1x_3 = x_2(x_1x_3 \vee \overline{x}_1) \vee \overline{x}_1x_3 = x_2(x_3 \vee \overline{x}_1) \vee \overline{x}_1x_3 = \overline{x}_1x_2 \vee x_2x_3 \vee \overline{x}_1x_3.$$

Таким образом, программа Pr_g^1 реализует функцию $g(x_1, x_2, x_3) \in G_1$.

Очевидно, ненадежность программы Pr_g^1 не больше ε, поскольку эта программа содержит только один ненадежный функциональный оператор. □

Лемма 3. *Если полный конечный базис содержит функцию $\varphi_2(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus 1$, то в этом базисе функцию $g(x_1, x_2, x_3) = x_1x_2 \vee x_2x_3 \vee x_1x_3 \in G_1$ можно реализовать неветвящейся программой Pr_g^2 с ненадежностью $N_\varepsilon(\mathrm{Pr}_g^2) \leqslant \varepsilon$:*

$$\begin{array}{l}
\mathrm{Pr}_g^2(x_1, x_2, x_3):\\
z = \varphi_2(x_1, x_2, x_3)\\
\mathrm{stop}(x_1)\\
z = x_3\\
\mathrm{stop}(x_2)\\
z = x_1.
\end{array}$$

Доказательство. Пусть B — полный конечный базис, $\varphi_2(x_1, x_2, x_3) \in B$. Нетрудно проверить, что $\varphi_2(x_1, x_2, x_3) = (x_1 \vee \overline{x}_2 \vee \overline{x}_3)(\overline{x}_1 \vee x_2 \vee x_3)$. По формуле (2) найдем функцию, которую вычисляет программа Pr_g^2:

$$\mathrm{Pr}_g^2(x_1, x_2, x_3) = \varphi_2(x_1, x_2, x_3)x_1 \vee \overline{x}_1(x_2x_3 \vee \overline{x}_2x_1) = \varphi_2(x_1, x_2, x_3)x_1 \vee \overline{x}_1x_2x_3 =$$
$$= (x_1 \vee \overline{x}_2 \vee \overline{x}_3)(\overline{x}_1 \vee x_2 \vee x_3)x_1 \vee \overline{x}_1x_2x_3 = x_1x_2 \vee x_1x_2\overline{x}_3 \vee x_1x_3 \vee x_1\overline{x}_2x_3 \vee \overline{x}_1x_2x_3 =$$
$$= x_1x_2 \vee x_1x_3 \vee \overline{x}_1x_2x_3 = x_1x_2 \vee x_2x_3 \vee x_1x_3.$$

Таким образом, программа Pr_g^2 реализует функцию $g(x_1, x_2, x_3) \in G_1$.

Очевидно, ненадежность программы Pr_g^2 не больше ε, поскольку она содержит только один ненадежный функциональный оператор. □

Обозначим через T_0 ([7], с. 33) класс всех булевых функций $f(x_1,\ldots,x_n)$, сохраняющих константу 0, т. е. функций, для которых выполнено равенство $f(0,\ldots,0)=0$.

Пусть B — полный конечный базис, тогда по теореме Поста о функциональной полноте [7] он содержит функцию f_{T_0}, которая не сохраняет константу 0, т. е. $f_{T_0}(0,\ldots,0)=1$ ($f_{T_0}\notin T_0$).

Лемма 4 ([7], с. 40)**.** *Любой полный конечный базис содержит такую функцию h, что $h(x,\ldots,x)\in\{1,\overline{x}\}$.*

Действительно, любой полный базис содержит функцию $f_{T_0}\notin T_0$, для которой верно равенство $f_{T_0}(0,0,...,0)=1$. Возможны два случая: 1) $f_{T_0}(1,1,...,1)$=0 или 2) $f_{T_0}(1,1,...,1)$=1. Следовательно, в первом случае $f_{T_0}(x,x,\ldots,x)=\overline{x}$, а во втором — $f_{T_0}(x,x,\ldots,x)\equiv 1$, т.е. $h=f_{T_0}$ и $h(x,\ldots,x)\in\{1,\overline{x}\}$.

Таким образом, в любом полном конечном базисе можно реализовать либо константу 1, либо $\overline{x}$, используя один функциональный элемент.

Лемма 5. *Если полный конечный базис содержит функцию $\varphi_3(x_1,x_2,x_3)=x_1x_2\oplus x_2x_3\oplus x_1x_3\oplus x_1\oplus x_2\oplus x_3$, то в этом базисе функцию $g(x_1,x_2,x_3)=x_1\overline{x}_2\vee\overline{x}_2\overline{x}_3\vee x_1\overline{x}_3\in G_1$ можно реализовать неветвящейся программой Pr_g^3 с ненадежностью $N_\varepsilon(\mathrm{Pr}_g^3)=\varepsilon$.*

Доказательство. Пусть B — полный конечный базис, $\varphi_3(x_1,x_2,x_3)\in B$. Нетрудно проверить, что $\varphi_3(x_1,x_2,x_3)=(x_1\vee x_2\vee x_3)(\overline{x}_1\vee\overline{x}_2\vee\overline{x}_3)$. По лемме 4 в базисе B содержится такая функция $h=f_{T_0}$, что либо $h(x,\ldots,x)=\overline{x}$, либо $h(x,\ldots,x)\equiv 1$. Поэтому будем рассматривать два варианта для Pr_g^3: (a) $h(x,\ldots,x)=\overline{x}$; (b) $h(x,\ldots,x)\equiv 1$.

(1) Пусть $h(x,\ldots,x)=\overline{x}$ (вариант (a)):

$$
\begin{array}{ll}
\mathrm{Pr}_g^3(x_1,x_2,x_3): & \mathrm{Pr}_g^3(x_1,x_2,x_3): \\
z=\varphi_3(x_1,x_2,x_3) & z=\varphi_3(x_1,x_2,x_3) \\
\mathrm{stop}(x_1) & \mathrm{stop}(x_1) \\
z=x_1 & z=x_1 \\
\mathrm{stop}(x_2) & \mathrm{stop}(x_2) \\
\mathrm{stop}(x_3) & \mathrm{stop}(x_3) \\
z=\overline{x}_1. & z=1. \\
\quad\text{(a)} & \quad\text{(b)}
\end{array}
$$

По формуле (2) найдем функцию, которую вычисляет Pr_g^3 (a):

$$
\begin{aligned}
\mathrm{Pr}_g^3(x_1,x_2,x_3)&=\varphi_3(x_1,x_2,x_3)x_1\vee\overline{x}_1(x_1x_2\vee\overline{x}_2(x_1x_3\vee\overline{x}_3\overline{x}_1))=\\
&=(x_1\vee x_2\vee x_3)(\overline{x}_1\vee\overline{x}_2\vee\overline{x}_3)x_1\vee\overline{x}_1\overline{x}_2\overline{x}_3=x_1\overline{x}_2\vee x_1\overline{x}_3\vee x_1x_2\overline{x}_3\vee x_1\overline{x}_2x_3\vee\overline{x}_1\overline{x}_2\overline{x}_3=\\
&=\overline{x}_2(x_1\vee\overline{x}_1\overline{x}_3)\vee\overline{x}_3(x_1\vee\overline{x}_1\overline{x}_2)=x_1\overline{x}_2\vee\overline{x}_2\overline{x}_3\vee x_1\overline{x}_3.
\end{aligned}
$$

Таким образом, программа Pr_g^3 реализует функцию $g(x_1,x_2,x_3)\in G_1$.

Вычислим вероятности ошибок программы Pr_g^3 на всевозможных входных наборах

$$\breve{\alpha}=(\alpha_1,\alpha_2,\alpha_3).$$

Отметим, что на наборах $(0,1,0)$, $(0,0,1)$ и $(0,1,1)$ вероятность ошибки равна нулю, так как stop-оператор $\mathrm{stop}(x_1)$ на этих наборах не срабатывает, но срабатывают либо $\mathrm{stop}(x_2)$, либо $\mathrm{stop}(x_3)$, а следовательно, ошибки функциональных операторов $z=\varphi_3(x_1,x_2,x_3)$ или $z=\overline{x}_1$ не влияют на результат работы программы Pr_g^3.

Пусть входной набор $\check{\alpha}$ равен одному из наборов $(1,0,0)$, $(1,0,1)$, $(1,1,0)$. Тогда срабатывает stop-оператор $\mathrm{stop}(x_1)$, выходное значение программы z при отсутствии неисправностей равно $\varphi_3(\check{\alpha})=1$, а вероятность ошибки $P_0(\mathrm{Pr}_g^3,\check{\alpha})=\varepsilon$. Аналогично на входном наборе $\check{\alpha}=(1,1,1)$ вероятность ошибки $P_1(\mathrm{Pr}_g^3,\check{\alpha})=\varepsilon$.

Пусть входной набор $\check{\alpha}=(0,0,0)$. Тогда ни один из трех stop-операторов не срабатывает, выходное значение программы z при отсутствии неисправностей равно $\overline{x}_1$ и единице. В этом случае вероятность ошибки $P_0(\mathrm{Pr}_g^3,\check{\alpha})=\varepsilon$.

Таким образом, $N_\varepsilon(\mathrm{Pr}_g^3)=\varepsilon$.

(2) Пусть $h(x,\dots,x)\equiv 1$ (вариант (b)). По формуле (2) найдем функцию, которую вычисляет Pr_g^3 (b):

$$\begin{aligned}\mathrm{Pr}_g^3(x_1,x_2,x_3)&=\varphi_3(x_1,x_2,x_3)x_1\vee\overline{x}_1(x_1x_2\vee\overline{x}_2(x_1x_3\vee\overline{x}_3\cdot 1))=\\&=(x_1\vee x_2\vee x_3)(\overline{x}_1\vee\overline{x}_2\vee\overline{x}_3)x_1\vee\overline{x}_1\overline{x}_2\overline{x}_3=x_1\overline{x}_2\vee x_1\overline{x}_3\vee x_1x_2\overline{x}_3\vee x_1\overline{x}_2x_3\vee\overline{x}_1\overline{x}_2\overline{x}_3=\\&=\overline{x}_2(x_1\vee\overline{x}_1\overline{x}_3)\vee\overline{x}_3(x_1\vee\overline{x}_1\overline{x}_2)=x_1\overline{x}_2\vee\overline{x}_2\overline{x}_3\vee x_1\overline{x}_3.\end{aligned}$$

Таким образом, Pr_g^3 реализует функцию $g(x_1,x_2,x_3)\in G_1$. Ненадежность программы Pr_g^3 (b) вычисляется так же, как в первом случае. □

Лемма 6. *Если полный конечный базис содержит функцию $\varphi_4(x_1,x_2,x_3)=x_1x_2\oplus x_2x_3\oplus x_1x_3\oplus x_1$, то в этом базисе функцию $g(x_1,x_2,x_3)=\overline{x}_1\overline{x}_2\vee\overline{x}_2x_3\vee\overline{x}_1x_3\in G_1$ можно реализовать неветвящейся программой Pr_g^4 с ненадежностью $N_\varepsilon(\mathrm{Pr}_g^4)=\varepsilon$.*

Доказательство. Пусть B — полный конечный базис, $\varphi_4(x_1,x_2,x_3)\in B$. Нетрудно проверить, что $\varphi_4(x_1,x_2,x_3)=\overline{x}_1x_2x_3\vee x_1\overline{x}_2\overline{x}_3$. По лемме 4 в базисе B содержится такая функция $h=f_{T_0}$, что либо $h(x,\dots,x)=\overline{x}$, либо $h(x,\dots,x)\equiv 1$. Поэтому будем рассматривать два варианта Pr_g^4: (a) $h(x,\dots,x)=\overline{x}$; (b) $h(x,\dots,x)\equiv 1$.

(1) Пусть $h(x,\dots,x)=\overline{x}$ (вариант (a)):

(a)	(b)
$\mathrm{Pr}_g^4(x_1,x_2,x_3):$	$\mathrm{Pr}_g^4(x_1,x_2,x_3):$
$z=\varphi_4(x_1,x_2,x_3)$	$z=\varphi_4(x_1,x_2,x_3)$
$\mathrm{stop}(x_2)$	$\mathrm{stop}(x_2)$
$z=x_3$	$z=x_3$
$\mathrm{stop}(x_3)$	$\mathrm{stop}(x_3)$
$z=\overline{x}_1.$	$\mathrm{stop}(x_1)$
	$z=1.$

По формуле (2) найдем функцию, которую вычисляет Pr_g^4 (a):

$$\begin{aligned}\mathrm{Pr}_g^4(x_1,x_2,x_3)&=\varphi_4(x_1,x_2,x_3)x_2\vee\overline{x}_2(x_3\vee\overline{x}_3\overline{x}_1)=\varphi_4(x_1,x_2,x_3)x_2\vee\overline{x}_2(x_3\vee\overline{x}_1)=\\&=\overline{x}_1x_2x_3\vee\overline{x}_2x_3\vee\overline{x}_1\overline{x}_2=x_3(\overline{x}_1x_2\vee\overline{x}_2)\vee\overline{x}_1\overline{x}_2=x_3(\overline{x}_1\vee\overline{x}_2)\vee\overline{x}_1\overline{x}_2=\overline{x}_1\overline{x}_2\vee\overline{x}_2x_3\vee\overline{x}_1x_3.\end{aligned}$$

Таким образом, Pr_g^4 реализует функцию $g(x_1,x_2,x_3)\in G_1$.

Вычислим вероятности ошибок программы Pr_g^4 на всевозможных входных наборах $\check{\alpha}=(\alpha_1,\alpha_2,\alpha_3)$.

Отметим, что на наборах $(0,0,1)$ и $(1,0,1)$ вероятность ошибки равна нулю, так как stop-оператор $\mathrm{stop}(x_2)$ на этих наборах не срабатывает, но срабатывает $\mathrm{stop}(x_3)$, а следовательно, ошибки функциональных операторов $z = \varphi_4(x_1, x_2, x_3)$ или $z = \overline{x}_1$ не влияют на результат работы программы Pr_g^4.

Пусть входной набор $\breve{\alpha}$ равен одному из наборов $(0,1,0)$, $(1,1,0)$, $(1,1,1)$. Тогда срабатывает $\mathrm{stop}(x_2)$, выходное значение программы z при отсутствии неисправностей равно $\varphi_4(\breve{\alpha}) = 0$, а вероятность ошибки $P_1(\mathrm{Pr}_g^4, \breve{\alpha}) = \varepsilon$. Аналогично на входном наборе $\breve{\alpha} = (0,1,1)$ вероятность ошибки $P_0(\mathrm{Pr}_g^4, \breve{\alpha}) = \varepsilon$.

Пусть входной набор $\breve{\alpha} = (1,0,0)$. Тогда ни один из двух stop-операторов не срабатывает, выходное значение программы z при отсутствии неисправностей равно нулю. В этом случае вероятность ошибки $P_1(\mathrm{Pr}_g^4, \breve{\alpha}) = \varepsilon$. Аналогично на входном наборе $\breve{\alpha} = (0,0,0)$ вероятность ошибки $P_0(\mathrm{Pr}_g^4, \breve{\alpha}) = \varepsilon$.

Таким образом, $N_\varepsilon(\mathrm{Pr}_g^4) = \varepsilon$.

(2) Пусть $h(x, \ldots, x) \equiv 1$ (вариант (b)):

$$\mathrm{Pr}_g^4(x_1, x_2, x_3) = \varphi_4(x_1, x_2, x_3)x_2 \vee \overline{x}_2(x_3 \vee \overline{x}_3(x_3x_1 \vee \overline{x}_1 \cdot 1)) =$$
$$= \varphi_4(x_1, x_2, x_3)x_2 \vee \overline{x}_2(x_3 \vee \overline{x}_3\overline{x}_1) = \varphi_4(x_1, x_2, x_3)x_2 \vee \overline{x}_2(x_3 \vee \overline{x}_1) = \overline{x}_1x_2x_3 \vee \overline{x}_2x_3 \vee \overline{x}_1\overline{x}_2 =$$
$$= x_3(\overline{x}_1x_2 \vee \overline{x}_2) \vee \overline{x}_1\overline{x}_2 = x_3(\overline{x}_1 \vee \overline{x}_2) \vee \overline{x}_1\overline{x}_2 = \overline{x}_1\overline{x}_2 \vee \overline{x}_2x_3 \vee \overline{x}_1x_3.$$

Таким образом, Pr_g^4 реализует функцию $g(x_1, x_2, x_3) \in G_1$. Ненадежность программы Pr_g^4 (b) вычисляется так же, как в первом случае. □

Лемма 7. *Пусть B – полный конечный базис, а программа Pr_g реализует в этом базисе некоторую функцию $g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$ $(a_i \in \{0,1\}, i \in \{1,2,3\})$ с ненадежностью $N_\varepsilon(\mathrm{Pr}_g)$. Тогда любую булеву функцию f в этом базисе можно реализовать программой Pr_f, ненадежность которой при всех $\varepsilon \in (0, 1/960]$ удовлетворяет неравенству*

$$N_\varepsilon(\mathrm{Pr}_f) \leqslant N_\varepsilon(\mathrm{Pr}_g) + 81\varepsilon^2.$$

Доказательство. Пусть программа Pr_g реализует некоторую функцию $g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$ $(a_i \in \{0,1\}, i \in \{1,2,3\})$. Обозначим через f^a функцию f, если $a = 1$, и функцию $\overline{f}$, если $a = 0$. По теореме 1 функцию f^{a_i} $(i \in \{1,2,3\})$ можно реализовать схемой S_i, функционирующей с ненадежностью $N_\varepsilon(S_i) \leqslant 5\varepsilon + 182\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$. Обозначим $P = 5\varepsilon + 182\varepsilon^2$. Используя по одному экземпляру схем S_1, S_2 и S_3 и программу $\mathrm{Pr}_g(x_1, x_2, x_3)$, для функции f построим неветвящуюся программу

Pr_f :
$y_1 = f^{a_1}[S_1]$
$y_2 = f^{a_2}[S_2]$
$y_3 = f^{a_3}[S_3]$
$\mathrm{Pr}_g(y_1, y_2, y_3)$.

Пусть $\widetilde{\beta}$ — произвольный входной набор программы Pr_f, а $P(S_i, \widetilde{\beta})$ — вероятности ошибок на выходах схем S_i $(i \in \{1,2,3\})$ соответственно при $\widetilde{\beta}$. Обозначим $P_i = P(S_i, \widetilde{\beta})$, $i \in \{1,2,3\}$. Очевидно, $\max\{P_1, P_2, P_3\} \leqslant \{N_\varepsilon(S_1), N_\varepsilon(S_2), N_\varepsilon(S_3)\} \leqslant P$. На наборе $\widetilde{\beta}$ оценим вероятность ошибки

$$P(\mathrm{Pr}_f, \widetilde{\beta}) \leqslant (1 - P_1)(1 - P_2)(1 - P_3) \cdot N(\mathrm{Pr}_g)+$$
$$+ [P_1(1 - P_2)(1 - P_3) + (1 - P_1)P_2(1 - P_3) + (1 - P_1)(1 - P_2)P_3] \cdot N(\mathrm{Pr}_g)+$$
$$+ [P_1P_2(1 - P_3) + (1 - P_1)P_2P_3 + P_1(1 - P_2)P_3] \cdot 1 + P_1P_2P_3 \cdot 1 =$$

$$
\begin{gathered}
=[(1-P_2)(1-P_3)+(1-P_1)P_2(1-P_3)+(1-P_1)(1-P_2)P_3]\cdot N(\mathrm{Pr}_g)+\\
+[P_1P_2+(1-P_1)P_2P_3+P_1(1-P_2)P_3]\leqslant\\
\leqslant[(1-P_3)(1-P_1P_2)+(1-P_1)(1-P_2)P_3]\cdot N(\mathrm{Pr}_g)+[P_1P_2+P_2P_3+P_1P_3]\leqslant\\
\leqslant[1\underbrace{-P_1P_2}_{<0}+P_3\underbrace{(2P_1P_2-P_1-P_2)}_{<0}]\cdot N(\mathrm{Pr}_g)+3P^2\leqslant N(\mathrm{Pr}_g)+3P^2.
\end{gathered}
$$

Подставляя в последнее неравенство значение P и учитывая условие $\varepsilon\in(0,1/960]$, получим $P(\mathrm{Pr}_f,\widetilde{\beta})\leqslant N_\varepsilon(\mathrm{Pr}_g)+81\varepsilon^2$. Тогда $N_\varepsilon(\mathrm{Pr}_f)=\max\limits_{\widetilde{\beta}}P(\mathrm{Pr}_f,\widetilde{\beta})\leqslant\max\limits_{\widetilde{\beta}}(N_\varepsilon(\mathrm{Pr}_g)+81\varepsilon^2)$, т. е. $N_\varepsilon(\mathrm{Pr}_f)\leqslant N_\varepsilon(\mathrm{Pr}_g)+81\varepsilon^2$. □

4. Доказательство теоремы 6

Пусть B — полный конечный базис с некоторой особенной функцией $\varphi(x_1,x_2,x_3)=x_1x_2\oplus x_1x_3\oplus x_2x_3\oplus c_1x_1\oplus c_2x_2\oplus c_3x_3\oplus c_0$ $(c_0,c_1,c_2,c_3\in\{0,1\})$. Возможны два случая: функция $\varphi(x_1,x_2,x_3)$ конгруэнтна функции вида $x_1x_2\oplus x_2x_3\oplus x_1x_3\oplus c_1(x_2\oplus x_3)\oplus c_2$ или $x_1x_2\oplus x_2x_3\oplus x_1x_3\oplus x_1\oplus c_1(x_2\oplus x_3)\oplus c_2$ $(c_1,c_2\in\{0,1\})$.

В первом случае легко проверить, что $\varphi(x_1,x_2,x_3)\in G_1$. Тогда применима теорема 2 (поскольку схему из функциональных элементов можно считать частным случаем неветвящейся программы), по которой любую булеву функцию можно реализовать неветвящейся программой с ненадежностью, не большей $\varepsilon+8\varepsilon^2$ при всех $\varepsilon\in(0,1/960]$, т. е. утверждение теоремы 6 верно.

Пусть теперь базис B содержит функцию $\varphi(x_1,x_2,x_3)$, конгруэнтную функции вида $x_1x_2\oplus x_2x_3\oplus x_1x_3\oplus x_1\oplus c_1(x_2\oplus x_3)\oplus c_2$ $(c_1,c_2\in\{0,1\})$. Возможны четыре варианта: 1) $c_1=c_2=1$; 2) $c_1=0$, $c_2=1$; 3) $c_1=1$, $c_2=0$; 4) $c_1=c_2=0$.

В каждом из этих случаев по леммам 2, 3, 5 и 6 соответственно можно реализовать некоторую функцию $g(x_1,x_2,x_3)=x_1^{a_1}x_2^{a_2}\vee x_1^{a_1}x_3^{a_3}\vee x_2^{a_2}x_3^{a_3}$ $(a_i\in\{0,1\},\ i\in\{1,2,3\})$ программой Pr_g, ненадежность которой $N_\varepsilon(\mathrm{Pr}_g)\leqslant\varepsilon$. Отметим, что значения параметров a_i $(i=1,2,3)$ во всех четырех случаях различны и соответственно равны: 1) $a_1=0$, $a_2=a_3=1$; 2) $a_1=a_2=a_3=1$; 3) $a_1=1$, $a_2=a_3=0$; 4) $a_1=a_2=0$, $a_3=1$.

Пусть f — любая булева функция. Воспользуемся леммой 7, выбирая значения a_1, a_2, a_3 в каждом из четырех случаев соответствующим образом. Тогда функцию f можно реализовать неветвящейся программой, которая функционирует с ненадежностью, не большей $\varepsilon+81\varepsilon^2$ при $\varepsilon\in(0,1/960]$. □

Цель дальнейших исследований авторов — получить нижние оценки ненадежности неветвящихся программ.

Литература

[1] Чашкин А.В. *О среднем времени вычисления значений булевых функций*, Дискретн. анализ и исследов. операций (Новосибирск, 1997), Сер. 1 **4** (1), 60–78.

[2] Чашкин А.В. *Лекции по дискретной математике.* Учеб. пособие (МГУ, мехмат, М., 2007).

[3] Алехина М.А., Васин А.В. *О надежности схем в базисах, содержащих функции не более чем трех переменных*, Учен. зап. Казанск. ун-та. Сер. Физ.-матем. науки **151** (2), 25–35 (2009).

[4] Васин А.В. *Об асимптотически оптимальных схемах в базисе $\{x_1\&x_2,\overline{x}_1\}$ при инверсных неисправностях на выходах элементов*, Дискретн. анализ и исследов. операций (Новосибирск, 2009) **16** (6), 12–22.

[5] Васин А.В. *Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов*, Дисс. … канд. физ.-матем. наук (Пенза, 2010).

[6] Редькин Н.П. *О полных проверяющих тестах для схем из функциональных элементов*, Матем. вопр. кибернетики (Наука, М., 1989), вып. 2, 198–222.

[7] Яблонский С.В. *Введение в дискретную математику: Учебное пособие для вузов*, Под ред. В.А. Садовничего, 3-е изд. (Высш. школа, М., 2001).

[8] Грабовская С.М. *О надежности неветвящихся программ в базисе, содержащем функцию вида* $x_1^{a_1} \vee x_2^{a_2}$, Изв. вузов. Поволжский регион. Физико-математические науки (ИИЦ ПГУ, Пенза, 2010), №4, 31–46.

[9] Грабовская С.М. *О надежности неветвящихся программ в базисе, содержащем функцию вида* $x_1^{a_1} \& x_2^{a_2}$, Дискретн. анализ и исследов. операций (Новосибирск, 2012) **19** (1), 49–56.

М.А. Алехина

профессор, заведующая кафедрой дискретной математики,
Пензенский государственный университет,
ул. Красная, д. 40, г. Пенза, 440026, Россия,

`e-mail:` alehina@pnzgu.ru

С.М. Грабовская

аспирант, кафедра дискретной математики,
Пензенский государственный университет,
ул. Красная, д. 40, г. Пенза, 440026, Россия,

`e-mail:` swetazin@mail.ru

M.A. Alekhina

Professor, Head of the Chair of Discrete Mathematics,
Penza State University,
40 Krasnaya str., Penza, 440026 Russia,

`e-mail:` alehina@pnzgu.ru

S.M. Grabovskaya

Postgraduate, Chair of Discrete Mathematics,
Penza State University,
40 Krasnaya str., Penza, 440026 Russia,

`e-mail:` swetazin@mail.ru