

УДК 519.718

О НАДЁЖНОСТИ НЕВЕТВЯЩИХСЯ ПРОГРАММ В БАЗИСЕ, СОДЕРЖАЩЕМ ОБОБЩЁННУЮ КОНЪЮНКЦИЮ *)

С. М. Грабовская

Аннотация. Рассматривается реализация булевых функций неветвящимися программами с операторами условной остановки в полном конечном базисе, содержащем хотя бы одну из функций $x_1 \cdot x_2$, $\bar{x}_1 \cdot x_2$ или $\bar{x}_1 \cdot \bar{x}_2$. Предполагается, что функциональные операторы с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах, а операторы условной остановки абсолютно надёжны. Доказано, что в таких базисах любую булеву функцию можно реализовать неветвящейся программой, функционирующей с ненадёжностью не больше $\varepsilon + 59\varepsilon^2$ при $\varepsilon \in (0, 1/960]$.

Ключевые слова: булева функция, неветвящаяся программа, оператор условной остановки, синтез, надёжность.

Введение

Рассматривается реализация булевых функций неветвящимися программами с операторами условной остановки [4] в полном конечном базисе B . Программы с оператором условной остановки характеризуются наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы при выполнении определённого условия. Сформулируем необходимые понятия и определения [4].

Пусть $X = \{x_1, \dots, x_n\}$ — множество независимых булевых переменных, $\tilde{x} = (x_1, \dots, x_n)$ — набор независимых переменных, $n \in \mathbb{N}$. Введём множества переменных $Y = \{y_1, \dots, y_l\}$ и $Z = \{z_1, \dots, z_m\}$, $l, m \in \mathbb{N}$. Переменные из Y назовём *внутренними*, а из Z — *выходными* переменными. Пусть $a \in Y \cup Z$, $b_1, \dots, b_d \in X \cup Y \cup Z$ ($d \in \{1, \dots, n\}$), h — булева функция из базиса B , зависящая не более чем от d переменных. *Вычислительным оператором* p назовём выражение $p : a = h(b_1, \dots, b_d)$. Переменную a назовём *выходом вычислительного оператора*, переменные b_1, \dots, b_d — *её входами*.

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

Пусть $a \in X \cup Y \cup Z$. Оператором остановки p назовём выражение $p : \text{Stop}(a)$. Переменную a назовём *выходом* оператора остановки p .

Последовательность $\text{Pr} = p_1 \dots p_i \dots p_L$, состоящая из вычислительных операторов и операторов остановки, называется *неветвящейся программой с условной остановкой*, если при любом $j \in \{1, 2, \dots, L\}$ каждый вход оператора p_j есть либо независимая переменная, либо выход некоторого вычислительного оператора.

Неветвящаяся программа работает в дискретные моменты времени $t = 0, 1, 2, \dots$, не изменяет значений независимых переменных и изменяет значения внутренних и выходных переменных. Значения $y_i(\tilde{x}; t)$ внутренних переменных y_i и $z_j(\tilde{x}; t)$ выходных переменных z_j программы Pr в произвольный момент времени t на наборе независимых переменных $\tilde{x} = (x_1, \dots, x_n)$ определим индуктивно следующим образом:

- (i) в начальный момент времени $t = 0$ значения всех внутренних и выходных переменных считаем неопределёнными;
- (ii) если оператор p_t не изменяет значения внутренней переменной y_i или выходной переменной z_j , то полагаем

$$y_i(\tilde{x}; t) = y_i(\tilde{x}; t - 1), \quad z_j(\tilde{x}; t) = z_j(\tilde{x}; t - 1);$$

- (iii) если оператор p_t изменяет значение внутренней переменной y_i или выходной переменной z_j и значения 1-го, \dots , d -го входов оператора p_t в момент времени $t - 1$ равны $b_1(\tilde{x}; t - 1), \dots, b_d(\tilde{x}; t - 1)$ соответственно, то полагаем

$$y_i(\tilde{x}; t) = h_t(b_1(\tilde{x}; t - 1), \dots, b_d(\tilde{x}; t - 1)),$$

$$z_j(\tilde{x}; t) = h_t(b_1(\tilde{x}; t - 1), \dots, b_d(\tilde{x}; t - 1)).$$

Значением оператора p_t программы Pr на наборе $\tilde{x} = (x_1, \dots, x_n)$ независимых переменных x_1, x_2, \dots, x_n назовём значение её выхода в момент времени t , обозначим его через $p_t(\tilde{x})$. Через $n(p)$ обозначим номер оператора p в программе Pr , т.е. $n(p_i) = i$. Пусть p_{t_1}, \dots, p_{t_r} — все операторы остановки из Pr , причём $t_1 < \dots < t_r$. Через s_j будем обозначать j -й оператор остановки программы Pr , т.е. $s_j \equiv p_{t_j}$. Вычислительный оператор p_i (переменную x_l) назовём *аргументом оператора остановки* s_j , $n(s_j) = r$, и обозначим через q_j , если (а) выход оператора p_i (переменная x_l) является входом оператора s_j , (б) среди p_t , $i < t < r$, нет оператора, выход которого совпадает с выходом p_i .

Будем говорить, что k -й оператор остановки s_k *прекращает вычисления программы* Pr на наборе \tilde{x} , если

$$q_1(\tilde{x}) = \dots = q_{k-1}(\tilde{x}) = 0, \quad q_k(\tilde{x}) = 1.$$

Результат действия программы Pr на наборе \tilde{x} обозначим через $\text{Pr}(\tilde{x})$ и его l -ю компоненту $\text{Pr}_l(\tilde{x})$ определим следующим образом:

$$\text{Pr}_l(\tilde{x}) = \begin{cases} z_l(\tilde{x}; t_k), & \text{если } q_1(\tilde{x}) = \dots = q_{k-1}(\tilde{x}) = 0, \ q_k(\tilde{x}) = 1, \\ z_l(\tilde{x}; L), & \text{если } q_1(\tilde{x}) = \dots = q_r(\tilde{x}) = 0, \end{cases}$$

т. е. $\text{Pr}_l(\tilde{x})$ равно значению l -й выходной переменной z_l в момент останова программы. Легко видеть, что

$$\begin{aligned} \text{Pr}_l(\tilde{x}) = & q_1(\tilde{x})z_l(\tilde{x}; t_1) \vee \bar{q}_1(\tilde{x})q_2(\tilde{x})z_l(\tilde{x}; t_2) \vee \dots \vee \bar{q}_1(\tilde{x})\bar{q}_2(\tilde{x}) \dots \\ & \bar{q}_{k-1}(\tilde{x})q_k(\tilde{x})z_l(\tilde{x}; t_k) \vee \dots \vee \bar{q}_1(\tilde{x})\bar{q}_2(\tilde{x}) \dots \bar{q}_{r-1}(\tilde{x})q_r(\tilde{x})z_l(\tilde{x}; t_r) \vee \dots \\ & \vee \bar{q}_1(\tilde{x})\bar{q}_2(\tilde{x}) \dots \bar{q}_r(\tilde{x})z_l(\tilde{x}; L). \end{aligned} \quad (1)$$

Иногда (1) удобнее использовать в преобразованном виде:

$$\begin{aligned} \text{Pr}_l(\tilde{x}) = & q_1(\tilde{x})z_l(\tilde{x}; t_1) \vee \bar{q}_1(\tilde{x})(q_2(\tilde{x})z_l(\tilde{x}; t_2) \vee \bar{q}_2(\tilde{x})(\dots \\ & (q_{k-1}(\tilde{x})z_l(\tilde{x}; t_{k-1}) \vee \bar{q}_{k-1}(\tilde{x})(\dots \vee \bar{q}_{r-1}(\tilde{x})(q_r(\tilde{x})z_l(\tilde{x}; t_r) \\ & \vee \bar{q}_r(\tilde{x})z_l(\tilde{x}; L)) \dots)) \dots)). \end{aligned} \quad (2)$$

Если $\text{Pr}(\tilde{x}) = f(\tilde{x})$ для любого \tilde{x} из $\{0, 1\}^n$, то программа Pr вычисляет n -местную булеву функцию f . Далее будем считать, что операторы условной остановки абсолютно надёжны, а вычислительные операторы базиса B независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах. Поскольку оператор условной остановки абсолютно надёжен, он срабатывает, когда на его вход поступает единица. Инверсные неисправности на выходах вычислительных операторов характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему функцию φ , а в неисправном — функцию $\bar{\varphi}$.

Программа Pr реализует булеву функцию $f(x_1, \dots, x_n)$, если она реализует её при отсутствии неисправностей.

Ненадёжностью $N(\text{Pr})$ программы Pr назовём максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах.

Чтобы использовать известные результаты для схем из функциональных элементов введём понятия ненадёжности схемы и асимптотически оптимальной схемы.

Ненадёжностью $N(S)$ схемы S из функциональных элементов, подверженных инверсным неисправностям на выходах, назовём максимальную вероятность ошибки на выходе схемы S при всевозможных входных наборах схемы S и обозначим её через $N_\varepsilon(f) = \inf N(S)$, где инфимум

берётся по всем схемам S из ненадёжных элементов, реализующим булеву функцию f .

Схема A из ненадёжных элементов, реализующая функцию f , называется *асимптотически оптимальной по надёжности*, если $N(A) \sim N_\varepsilon(f)$ при $\varepsilon \rightarrow 0$, т. е. $\lim_{\varepsilon \rightarrow 0} \frac{N_\varepsilon(f)}{N(A)} = 1$.

Теорема 1 [1]. В произвольном полном конечном базисе B любую булеву функцию f можно реализовать схемой S с ненадёжностью

$$N(S) \leq 5\varepsilon + 182\varepsilon^2 \quad \text{при } \varepsilon \in (0, 1/960].$$

Константа 5 в оценке ненадёжности из теоремы 1 в некоторых базисах, например, в $B = \{x_1 \& x_2, \bar{x}_1\}$, не может быть понижена [3].

1. О надёжности неветвящихся программ в базисах, содержащих функцию $x_1 \& x_2$

Пусть полный конечный базис B содержит $x_1 \& x_2$. Для неветвящихся программ с оператором условной остановки справедлива

Теорема 2. В полном конечном базисе B , содержащем $x_1 \& x_2$, при любом $n \in \mathbb{N}$ любую функцию $f(x_1, \dots, x_n)$ можно реализовать такой программой Pr_f^* , что $N(\text{Pr}_f^*) \leq \varepsilon + 54\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

ДОКАЗАТЕЛЬСТВО. Пусть полный конечный базис B содержит функцию $x_1 \& x_2$, $f(x_1, \dots, x_n)$ — произвольная булева функция, $n \in \mathbb{N}$. По теореме 1 её можно реализовать схемой S , которая при $\varepsilon \in (0, 1/960]$ функционирует с ненадёжностью $N(S) \leq 5\varepsilon + 182\varepsilon^2$. Используя четыре экземпляра схемы S , построим для f неветвящуюся программу Pr_f^* с абсолютно надёжными операторами условной остановки:

$$\text{Pr}_f^* : \left. \begin{array}{l} y_1 = f[S] \\ y_2 = f[S] \\ z = y_1 \& y_2 \\ \text{Stop}(z) \end{array} \right\} \text{Pr}_f^{*I} \left. \begin{array}{l} y_3 = f[S] \\ y_4 = f[S] \\ z = y_3 \\ \text{Stop}(y_4) \\ z = y_4 \end{array} \right\} \text{Pr}_f^{*II} \left. \begin{array}{l} \end{array} \right\} \text{Pr}_f^{*III}$$

Используя (2), найдём функцию, которую вычисляет программа Pr_f^* :

$$\begin{aligned}\text{Pr}_f^* &= y_1 y_2 \cdot y_1 y_2 \vee \overline{y_1 y_2} \cdot (y_3 y_4 \vee \overline{y_3 y_4}) = y_1 y_2 \vee \overline{y_1 y_2} \cdot y_3 y_4 \\ &= y_1 y_2 \vee y_3 y_4 = f \cdot f \vee f \cdot f = f.\end{aligned}$$

Следовательно, программа Pr_f^* реализует функцию f .

Программа Pr_f^* имеет один выход. Выделим в ней подпрограммы Pr_f^{*I} , Pr_f^{*II} и Pr_f^{*III} . Если срабатывает первый оператор остановки $\text{Stop}(z)$, то выполнение программы прекращается и на выходе программы $z = y_1 \& y_2$, если срабатывает второй $\text{Stop}(y_4)$, то $z = y_3$. При этом результат работы программы совпадает с результатом работ подпрограмм Pr_f^{*I} или Pr_f^{*II} соответственно. Если ни один из стоп-операторов не срабатывает, то выполнение программы продолжается и на выход идёт $z = y_4$. Результат работы программы совпадает с результатом работы подпрограммы Pr_f^{*III} .

Вычислим и оценим вероятности ошибок на выходе программы Pr_f^* . Пусть входной набор \tilde{a} такой, что $f(\tilde{a}) = 0$. Обозначим через $P_1(S, \tilde{a})$ вероятность ошибки схемы S на наборе \tilde{a} . Тогда

$$\begin{aligned}P_1(\text{Pr}_f^*, \tilde{a}) &= (1 - P_1(S, \tilde{a}))^2 \cdot \{\varepsilon + (1 - \varepsilon) \cdot P_1^2(S, \tilde{a})\} \\ &\quad + 2P_1(S, \tilde{a})(1 - P_1(S, \tilde{a})) \cdot \{\varepsilon + (1 - \varepsilon) \cdot P_1^2(S, \tilde{a})\} \\ &\quad + P_1^2(S, \tilde{a}) \cdot \{(1 - \varepsilon) + \varepsilon \cdot P_1^2(S, \tilde{a})\} \leq \varepsilon + 2N^2(S).\end{aligned}$$

Поскольку $N(S) \leq 5\varepsilon + 182\varepsilon^2$ и $\varepsilon \in (0, 1/960]$, получаем неравенство

$$P_1(\text{Pr}_f^*, \tilde{a}) \leq \varepsilon + 54\varepsilon^2. \quad (3)$$

Пусть набор \tilde{a} такой, что $f(\tilde{a}) = 1$. Обозначим через $P_0(S, \tilde{a})$ вероятность ошибки схемы S на наборе \tilde{a} . Тогда

$$\begin{aligned}P_0(\text{Pr}_f^*, \tilde{a}) &= (1 - P_0(S, \tilde{a}))^2 \cdot \varepsilon \cdot \{2P_0(S, \tilde{a})(1 - P_0(S, \tilde{a})) + P_0^2(S, \tilde{a})\} \\ &\quad + 2P_0(S, \tilde{a})(1 - P_0(S, \tilde{a})) \cdot (1 - \varepsilon) \cdot \{2P_0(S, \tilde{a})(1 - P_0(S, \tilde{a})) + P_0^2(S, \tilde{a})\} \\ &\quad + P_0^2(S, \tilde{a}) \cdot (1 - \varepsilon) \cdot \{2P_0(S, \tilde{a})(1 - P_0(S, \tilde{a})) + P_0^2(S, \tilde{a})\} \\ &\leq 2N(S)\varepsilon + 4N^2(S).\end{aligned}$$

Поскольку $N(S) \leq 5\varepsilon + 182\varepsilon^2$ и $\varepsilon \in (0, 1/960]$, получаем

$$P_0(\text{Pr}_f^*, \tilde{a}) \leq 118\varepsilon^2.$$

Отсюда и из (3) следует, что $N(\text{Pr}_f^*) \leq \varepsilon + 54\varepsilon^2$. Теорема 2 доказана.

2. О надёжности неветвящихся программ в базисах, содержащих функцию $\bar{x}_1 \& x_2$

Пусть полный конечный базис B содержит $\bar{x}_1 \& x_2$. Для неветвящихся программ с оператором условной остановки справедлива

Теорема 3. *В полном конечном базисе B , содержащем $\bar{x}_1 \& x_2$, при любом $n \in \mathbb{N}$ любую функцию $f(x_1, \dots, x_n)$ можно реализовать такой программой Pr_f^{**} , что $N(\text{Pr}_f^{**}) \leq \varepsilon + 54\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

ДОКАЗАТЕЛЬСТВО аналогично доказательству теоремы 2 с использованием программы Pr_f^{**} (рис. 1).

$\text{Pr}_f^{**} :$	$\text{Pr}_f^{***} :$
$y_1 = \bar{f}[S']$	$y_1 = \bar{f}[S']$
$y_2 = f[S]$	$y_2 = f[S']$
$z = \bar{y}_1 \& y_2$	$z = \bar{y}_1 \& \bar{y}_2$
$\text{Stop}(z)$	$\text{Stop}(z)$
$y_3 = \bar{f}[S']$	$y_3 = \bar{f}[S']$
$\text{Stop}(y_3)$	$\text{Stop}(y_3)$
$y_4 = f[S]$	$y_4 = \bar{f}[S']$
$z = y_4$	$z = \bar{y}_4 \& \bar{y}_4$

Рис. 1

Замечание 1. Теорема 3 справедлива для полных конечных базисов, содержащих $x_1 \& \bar{x}_2$, поскольку $x_1 \& \bar{x}_2$ получается из функции $\bar{x}_1 \& x_2$ переименованием переменных x_1 на x_2 и x_2 на x_1 .

3. О надёжности неветвящихся программ в базисах, содержащих функцию $\bar{x}_1 \& \bar{x}_2$

Пусть полный конечный базис B содержит $\bar{x}_1 \& \bar{x}_2$. Для неветвящихся программ с оператором условной остановки справедлива

Теорема 4. *В полном конечном базисе B , содержащем $\bar{x}_1 \& \bar{x}_2$, при любом $n \in \mathbb{N}$ любую функцию $f(x_1, \dots, x_n)$ можно реализовать такой программой Pr_f^{***} , что $N(\text{Pr}_f^{***}) \leq \varepsilon + 59\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

ДОКАЗАТЕЛЬСТВО аналогично доказательству теоремы 2 с использованием программы Pr_f^{***} (рис. 1).

Заключение

Из теорем 2, 3 и 4 с учётом замечания 1 следует

Теорема 5. В полном конечном базисе B , содержащем функцию вида $x_1^{a_1} \& x_2^{a_2}$ ($a_1, a_2 \in \{0, 1\}$), любую булеву функцию f можно реализовать такой программой Pr_f , что $N(\text{Pr}_f) \leq \varepsilon + 59\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.

Замечание 2. Утверждение теоремы 5 верно, если полный конечный базис содержит некоторую функцию вида $x_1^{a_1} \& x_2^{a_2} \& \dots \& x_k^{a_k}$ ($k \geq 3$, $a_i \in \{0, 1\}$, $i \in \{1, \dots, k\}$), поскольку, отождествляя некоторые переменные, из неё можно получить функцию вида $x_1^{b_1} \& x_2^{b_2}$, $b_1, b_2 \in \{0, 1\}$.

Из теоремы 5 следует, что в полном конечном базисе, содержащем хотя бы одну из функций $x_1 \cdot x_2$, $\bar{x}_1 \cdot x_2$ или $\bar{x}_1 \cdot \bar{x}_2$, любую булеву функцию f можно реализовать неветвящейся программой, ненадёжность которой не больше $\varepsilon + 59\varepsilon^2$ при $\varepsilon \in (0, 1/960]$.

Сравним полученный результат с известными результатами [2] для схем из функциональных элементов.

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

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

Пусть $B \subseteq B_3$ — полный базис. Обозначим $G = G_1 \cup G_2 \cup G_3$, где

$$G_1 = \{x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2^{\sigma_2} x_3^{\sigma_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\};$$

$$G_2 = \text{Congr}\{x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\};$$

$$G_3 = \text{Congr}\{x_1^{\sigma_1} x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2} x_3^{\sigma_3} \mid \sigma_i \in \{0, 1\}, i \in \{1, 2, 3\}\}.$$

Известно [1], что если полный конечный базис содержит функцию $\varphi \in G$, то любую функцию в этом базисе можно реализовать асимптотически оптимальной по надёжности схемой из функциональных элементов, ненадёжность которой асимптотически равна ε при $\varepsilon \rightarrow 0$. Если $B \subseteq B_3 \setminus G$, то для почти всех функций ненадёжность асимптотически оптимальных по надёжности схем асимптотически не меньше 2ε при $\varepsilon \rightarrow 0$ [1].

Например, для почти всех булевых функций можно построить асимптотически оптимальные по надёжности схемы с ненадёжностью, при $\varepsilon \rightarrow 0$ асимптотически равной 2ε в базисе $B = \{x_1 \& x_2, \bar{x}_1(x_2 \vee x_3), 1\}$ [2], 3ε в базисе $B = \{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$, 4ε в базисе $B = \{\bar{x}_1 \& x_2, \bar{x}_1\}$ [2] и 5ε в базисе $B = \{x_1 \& x_2, \bar{x}_1\}$ [3].

Итак, асимптотически оптимальные по надёжности схемы из функциональных элементов в различных полных базисах $B \subseteq B_3 \setminus G$, содержащих функции вида $x_1^{a_1} \& x_2^{a_2}$ ($a_1, a_2 \in \{0, 1\}$), имеют ненадёжность, асимптотически равную $k_B \cdot \varepsilon$ при $\varepsilon \rightarrow 0$, где константа k_B зависит от базиса B и $k_B \in \{2, 3, 4, 5\}$. При этом в любом полном конечном базисе, содержащем некоторую функцию вида $x_1^{a_1} \& x_2^{a_2}$ ($a_1, a_2 \in \{0, 1\}$), в том числе и в базисе $B' \subseteq B_3$, произвольную булеву функцию можно реализовать неветвящейся программой, функционирующей с ненадёжностью не больше $\varepsilon + 59\varepsilon^2$ при $\varepsilon \in (0, 1/960]$.

ЛИТЕРАТУРА

1. **Алехина М. А., Васин А. В.** О надёжности схем в базисах, содержащих функции не более чем трёх переменных // Уч. записки Казанского гос. ун-та. Сер. «Физ.-мат. науки». — Казань: Изд-во Казанск. ун-та, 2009. — Т. 151, вып. 2. — С. 25–35.
2. **Васин А. В.** Асимптотически оптимальные по надёжности схемы в полных базисах из трёхходовых элементов // Дисс. ... канд. физ.-мат. наук. — Пенза: Пензенский гос. ун-т, 2010. — 100 с.
3. **Васин А. В.** Об асимптотически оптимальных схемах в базисе $\{x_1 \& x_2, \bar{x}_1\}$ // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 6. — С. 12–22.
4. **Чашкин А. В.** О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. — 1997. — Т. 4, № 1. — С. 60–78.

Грабовская Светлана Михайловна,
e-mail: swetazin@mail.ru

Статья поступила
16 ноября 2010 г.

Переработанный вариант —
14 октября 2011 г.