

Ш.Е. БОЗОЯН, В.С. ЕГИАЗАРЯН, Д.А. КОЧАРОВ, Н.В. БАДАЛЯН

ПРИМЕНЕНИЕ БУЛЕВЫХ ДИФФЕРЕНЦИАЛОВ И АКТИВНОСТЕЙ ПЕРЕМЕННЫХ БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ВЫДЕЛЕНИЯ АКТИВНОЙ ЧАСТИ СХЕМЫ

Рассматриваются булевый дифференциал и его основные свойства, активность совокупности переменных булевой функции, а также комбинационная цифровая схема с одним выходом, реализующая булеву функцию. Используя активности входов комбинационной схемы и алгоритм построения активной части схемы для тестовых эталонных схем (ISCAS-85), выделяются активные части подсхем, имеющие один выход.

Ключевые слова: булевый дифференциал, проектирование, цифровая схема, активная часть.

Введение. В автоматизированном проектировании интегральных схем (ИС) контролирование правильности переходов от одного этапа проектирования к следующему осуществляется верификацией и тестированием промежуточных результатов. Эти процедуры настолько трудоемки, что поглощают около 80% временных ресурсов всего цикла проектирования ИС, из чего следует, что сокращение времени верификации и тестирования просто означает сокращение времени проектирования ИС. Трудоемкость указанных процедур обусловлена не только увеличением числа элементов в современных кристаллах, а в основном числом входов схем в кристаллах, число входных наборов которых растет экспоненциально относительно числа входов. Практическая недоступность использования всех входных наборов с целью проверки исправности проекта схемы заставляет из всех этих входных наборов подобрать наиболее «ценные» (в определенном смысле), использование которых позволяет наиболее эффективно осуществить проверку работоспособности схемы. Это очень трудная задача, тем более, что каждая схема диктует свои особенности подбора этих приемлемых входных наборов.

Выделение активной части булевой функции (соответственно – схемы с одним выходом) эффективным образом решает указанную проблему [1].

1. Производная. Понятие производной по отдельным переменным булевой функции ввел И.С. Рид [2] и применил при изучении общей схемы декодирования систематических кодов. Здесь рассматривается более общее понятие производной [3].

Определение 1. Производной булевой функции $f(x_1, \dots, x_{i_1}, \dots, x_{i_k}, \dots, x_n)$ по совокупности переменных $x_{i_1}, \dots, x_{i_k}$ называется функция

$$\frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_k})} = f(x_1, \dots, x_{i_1}, \dots, x_{i_k}, \dots, x_n) \oplus f(x_1, \dots, \bar{x}_{i_1}, \dots, \bar{x}_{i_k}, \dots, x_n),$$

где $\oplus$ - операция сложения по mod2.

Совокупность переменных $(x_{i_1}, \dots, x_{i_k})$ обозначим через A : $A = (x_{i_1}, \dots, x_{i_k})$ ($1 \leq i_1 < i_2 < \dots < i_k \leq n$), а также $\bar{A} = (\bar{x}_{i_1}, \dots, \bar{x}_{i_k})$ и, соответственно,

$$f(x_1, \dots, x_{i_1}, \dots, x_{i_k}, \dots, x_n) = f(x_1, \dots, A, \dots, x_n),$$

$$f(x_1, \dots, \bar{x}_{i_1}, \dots, \bar{x}_{i_k}, \dots, x_n) = f(x_1, \dots, \bar{A}, \dots, x_n).$$

Приведем некоторые легко проверяемые свойства:

1.1. Для любого A имеет место равенство: $\frac{\partial \bar{f}}{\partial A} = \frac{\partial f}{\partial A}.$

1.2. Булева функция $f(x_1, \dots, x_n)$ существенно не зависит от x_i тогда и только тогда, когда $\frac{\partial f}{\partial x_i} = 0.$

1.3. Для любых двух функций $f_1(x_1, \dots, x_n)$ и $f_2(x_1, \dots, x_n)$ и для любого A :

$$\begin{aligned} \text{а) } \frac{\partial(f_1 \oplus f_2)}{\partial A} &= \frac{\partial f_1}{\partial A} \oplus \frac{\partial f_2}{\partial A}, \\ \text{б) } \frac{\partial(f_1 f_2)}{\partial A} &= f_1 \frac{\partial f_2}{\partial A} \oplus f_2 \frac{\partial f_1}{\partial A} \oplus \frac{\partial f_1}{\partial A} \cdot \frac{\partial f_2}{\partial A}, \\ \text{в) } \frac{\partial(f_1 \vee f_2)}{\partial A} &= \bar{f}_1 \frac{\partial f_2}{\partial A} \oplus \bar{f}_2 \frac{\partial f_1}{\partial A} \oplus \frac{\partial f_1}{\partial A} \oplus \frac{\partial f_2}{\partial A}. \end{aligned}$$

1.4. $f(x_1, \dots, x_n) = x_i \frac{\partial f}{\partial x_i} \oplus f(x_1, \dots, x_{i-1}, 0 x_{i+1}, \dots, x_n).$

1.5.

$$\begin{aligned} \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_k})} &= \frac{\partial f(x_1, \dots, x_{i_1}, \dots, x_{i_2}, \dots, x_{i_{k-1}}, \dots, x_{i_k}, \dots, x_n)}{\partial x_{i_1}} \oplus \\ &\oplus \frac{\partial f(x_1, \dots, \bar{x}_{i_1}, \dots, x_{i_2}, \dots, x_{i_{k-1}}, \dots, x_{i_k}, \dots, x_n)}{\partial x_{i_2}} \oplus \\ &\oplus \dots \oplus \frac{\partial f(x_1, \dots, \bar{x}_{i_1}, \dots, \bar{x}_{i_2}, \dots, \bar{x}_{i_{k-1}}, \dots, x_{i_k}, \dots, x_n)}{\partial x_{i_k}}. \end{aligned}$$

Доказательство. Равенства 1.1 и 1.2 непосредственно следуют из определения 1.

1.3а.

$$\begin{aligned}\frac{\partial(f_1 \oplus f_2)}{\partial A} &= f_1(x_1, \dots, A, \dots, x_n) \oplus f_2(x_1, \dots, A, \dots, x_n) \oplus \\ &\oplus f_1(x_1, \dots, \bar{A}, \dots, x_n) \oplus f_2(x_1, \dots, \bar{A}, \dots, x_n) = \frac{\partial f_1}{\partial A} \oplus \frac{\partial f_2}{\partial A}.\end{aligned}$$

1.3б. Для доказательства этого равенства достаточно раскрыть правую часть, согласно определению 1, и упростить полученное выражение.

1.3в. Это равенство следует из равенства 1.3б, имея в виду известное равенство $f_1 \vee f_2 = \overline{\bar{f}_1 \cdot \bar{f}_2}$ и свойство 1.1.

Доказательство свойства 1.4 следует из цепочки равенств:

$$\begin{aligned}f(x_1, \dots, x_n) &= x_i f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \oplus \\ &\oplus \bar{x}_i f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = \\ &= x_i f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \oplus (1 \oplus x_i) f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = \\ &= x_i (f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \oplus f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)) \oplus \\ &\oplus f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = x_i \frac{\partial f}{\partial x_i} f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n).\end{aligned}$$

Идею доказательства свойства 1.5 продемонстрируем для $n=6$ и некоторой совокупности переменных. Рассмотрим функцию $f(x_1, \dots, x_6)$. Для совокупности переменных x_2, x_4, x_5 получим

$$\begin{aligned}\frac{\partial f}{\partial(x_2 x_4 x_5)} &= [f(x_1, x_2, x_3, x_4, x_5, x_6) \oplus f(x_1, \bar{x}_2, x_3, \bar{x}_4, \bar{x}_5, x_6)] = \\ &= [f(x_1, x_2, x_3, x_4, x_5, x_6) \oplus f(x_1, \bar{x}_2, x_3, x_4, x_5, x_6)] \oplus \\ &\oplus [f(x_1, \bar{x}_2, x_3, x_4, x_5, x_6) \oplus f(x_1, \bar{x}_2, x_3, \bar{x}_4, x_5, x_6)] \oplus \\ &\oplus [f(x_1, \bar{x}_2, x_3, \bar{x}_4, x_5, x_6) \oplus f(x_1, \bar{x}_2, x_3, \bar{x}_4, \bar{x}_5, x_6)] = \\ &= \frac{\partial f(x_1, x_2, x_3, x_4, x_5, x_6)}{\partial x_2} \oplus \frac{\partial f(x_1, \bar{x}_2, x_3, x_4, x_5, x_6)}{\partial x_4} \oplus \\ &\oplus \frac{\partial f(x_1, \bar{x}_2, x_3, \bar{x}_4, x_5, x_6)}{\partial x_5}.\end{aligned}$$

По индукции введем понятие повторной производной.

Определение 2. Базис индукции:

$$\frac{\partial^1 f}{\partial x_i} = \frac{\partial f}{\partial x_i}.$$

Индукционный шаг:

$$\frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_{k-1}} \partial x_{i_k}} = \frac{\partial}{\partial x_{i_k}} \left(\frac{\partial^{k-1} f}{\partial x_{i_1} \dots \partial x_{i_{k-1}}} \right), (k = 2, 3, \dots).$$

Повторная производная обладает следующими свойствами:

$$1.6. \frac{\partial^2 f}{\partial x_i \partial x_j} = \frac{\partial^2 f}{\partial x_j \partial x_i}, \text{ в общем случае}$$

$$\frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_m} \dots \partial x_{i_e} \dots \partial x_{i_k}} = \frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_e} \dots \partial x_{i_m} \dots \partial x_{i_k}}.$$

$$1.7. \frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_m} \dots \partial x_{i_m} \dots \partial x_{i_k}} = 0 \text{ и, в частности, } \frac{\partial^2 f}{\partial x_i \partial x_i} = 0.$$

Доказательство свойств 1.6 и 1.7 непосредственно следует из определений 1 и 2.

Следующие свойства устанавливают связь между производными по совокупности переменных и повторными производными.

1.8. Для любой функции $f(x_1, \dots, x_n)$ и любого набора индексов $i_1 < i_2 < \dots < i_k$ ($1 \leq i_j \leq n$, $j = \overline{1, k}$) справедливы равенства:

1.8a.

$$\begin{aligned} \frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_k}} &= \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_k})} \oplus \frac{\partial f}{\partial(x_{i_1}, \dots, \partial x_{i_{k-1}})} \oplus \dots \\ &\dots \oplus \frac{\partial f}{\partial(x_{i_2}, \dots, x_{i_k})} \oplus \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{k-2}})} \oplus \dots \oplus \frac{\partial f}{\partial(x_{i_3}, \dots, x_{i_k})} \oplus \dots \\ &\dots \oplus \frac{\partial f}{\partial(x_{i_1}, x_{i_2})} \oplus \frac{\partial f}{\partial(x_{i_1}, x_{i_3})} \oplus \dots \oplus \frac{\partial f}{\partial(x_{i_1}, x_{i_k})} \oplus \frac{\partial f}{\partial(x_{i_2}, x_{i_3})} \oplus \dots \\ &\dots \oplus \frac{\partial f}{\partial(x_{i_2}, x_{i_k})} \oplus \dots \oplus \frac{\partial f}{\partial(x_{i_{k-1}}, x_{i_k})} \oplus \frac{\partial f}{\partial x_{i_1}} \oplus \frac{\partial f}{\partial x_{i_2}} \oplus \dots \oplus \frac{\partial f}{\partial x_{i_k}}. \end{aligned}$$

1.86.

$$\begin{aligned} \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_k})} &= \frac{\partial^k f}{\partial x_{i_1} \dots \partial x_{i_k}} \oplus \frac{\partial^{k-1} f}{\partial x_{i_1} \dots \partial x_{i_{k-1}}} \oplus \dots \oplus \frac{\partial^{k-1} f}{\partial x_{i_2} \dots \partial x_{i_k}} \oplus \\ &\oplus \frac{\partial^{k-2} f}{\partial x_{i_1} \dots \partial x_{i_{k-2}}} \oplus \dots \oplus \frac{\partial^{k-2} f}{\partial x_{i_3} \dots \partial x_{i_k}} \oplus \dots \oplus \frac{\partial^2 f}{\partial x_{i_1} \partial x_{i_2}} \oplus \frac{\partial^2 f}{\partial x_{i_1} \partial x_{i_3}} \oplus \dots \\ &\dots \oplus \frac{\partial^2 f}{\partial x_{i_1} \partial x_{i_k}} \oplus \frac{\partial^2 f}{\partial x_{i_2} \partial x_{i_3}} \oplus \frac{\partial^2 f}{\partial x_{i_2} \partial x_{i_4}} \oplus \dots \oplus \frac{\partial^2 f}{\partial x_{i_2} \partial x_{i_k}} \oplus \dots \oplus \frac{\partial^2 f}{\partial x_{i_{k-1}} \partial x_{i_k}} \oplus \\ &\oplus \frac{\partial f}{\partial x_{i_1}} \oplus \frac{\partial f}{\partial x_{i_2}} \oplus \dots \oplus \frac{\partial f}{\partial x_{i_k}}. \end{aligned}$$

Доказательство равенства 1.8 а проведем индукцией по k. Для k=1 оно верно. Пусть оно верно и для k=m-1. По индуктивному предположению:

$$\begin{aligned} \frac{\partial^{m-1} f}{\partial x_{i_1} \dots \partial x_{i_{m-1}}} &= \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{m-1}})} \oplus \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{m-2}})} \oplus \dots \\ &\dots \oplus \frac{\partial f}{\partial(x_{i_2}, \dots, x_{i_{m-1}})} \oplus \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{m-3}})} \oplus \dots \oplus \frac{\partial f}{\partial(x_{i_3}, \dots, x_{i_{m-1}})} \oplus \dots \\ &\dots \oplus \frac{\partial f}{\partial(x_{i_1}, x_{i_2})} \oplus \frac{\partial f}{\partial(x_{i_1}, x_{i_3})} \oplus \dots \oplus \frac{\partial f}{\partial(x_{i_{m-2}}, x_{i_{m-1}})} \oplus \frac{\partial f}{\partial x_{i_1}} \oplus \frac{\partial f}{\partial x_{i_2}} \oplus \dots \oplus \frac{\partial f}{\partial x_{i_{m-1}}}. \end{aligned}$$

Дифференцируя обе части последнего равенства по x_m и имея в виду легко проверяемое равенство

$$\frac{\partial}{\partial x_{i_m}} \left(\frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{m-1}})} \right) = \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_m})} \oplus \frac{\partial f}{\partial(x_{i_1}, \dots, x_{i_{m-1}})} \oplus \frac{\partial f}{\partial x_{i_m}},$$

получим равенство 1.8а для k = m.

Аналогично доказывается 1.8б.

2. Активность аргументов булевой функции.

Определение 3. Нормой булевой функции $f(x_1, \dots, x_n)$ называется [3] число

$$\|f\| = 2^{-n} \sum_{(\alpha_1, \dots, \alpha_n)} f(\alpha_1, \dots, \alpha_n),$$

где сумма берется по всем 2^n наборам $(\alpha_1, \dots, \alpha_n)$ из нулей и единиц.

Норма обладает следующими легко проверяемыми свойствами [4]:

а) для любого набора $(\sigma_1, \dots, \sigma_n)$ из нулей и единиц имеет место равенство

$$\|f(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})\| = \|f(x_1, \dots, x_n)\|, \text{ где } x^1 = x, \quad x^0 = \bar{x};$$

$$\text{б) } \|\bar{f}\| = 1 - \|f\|;$$

в) для функций $\varphi(x_1, \dots, x_m)$ и $\psi(x_{m+1}, \dots, x_n)$:

$$\|\varphi\psi\| = \|\varphi\| \cdot \|\psi\|,$$

$$\|\varphi \vee \psi\| = \|\varphi\| + \|\psi\| - \|\varphi\| \cdot \|\psi\|,$$

$$\|\varphi \oplus \psi\| = \|\varphi\| + \|\psi\| - 2\|\varphi\| \cdot \|\psi\|.$$

Определение 4. Активностью совокупности переменных $A = (x_{i_1}, \dots, x_{i_k})$ ($1 \leq i_1 < i_2 < \dots < i_k \leq n$) функции $f(x_1, \dots, x_n)$ называется число

$$\omega_A^f = \left\| \frac{\partial f}{\partial A} \right\|.$$

Перечислим некоторые наиболее важные свойства активностей переменных [2,4,5]:

2.1. Для любого A $0 \leq \omega_A^f \leq 1$.

2.2. Функция $f(x_1, \dots, x_i, \dots, x_n)$ существенно не зависит от x_i тогда и только тогда, когда $\omega_i^f = 0$.

2.3. $\omega_i^f = 1$ тогда и только тогда, когда

$$f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) = x_i \oplus f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n).$$

Это следует из 1.4.

2.4. Для любого $A = (x_{i_1}, \dots, x_{i_k})$ ($1 \leq i_1 < i_2 < \dots < i_k \leq n$) и функций $\varphi(x_1, \dots, x_n)$ и $\psi(x_{n+1}, \dots, x_{n+m})$:

$$\text{а) } \omega_A^{\varphi+\psi} = \omega_A^\varphi, \quad \text{б) } \omega_A^{\varphi\psi} = \|\psi\| \omega_A^\varphi, \quad \text{в) } \omega_A^{\varphi \vee \psi} = \|\bar{\psi}\| \omega_A^\varphi.$$

2.5. Для любого A и любого набора $(\sigma_0, \sigma_1, \dots, \sigma_n)$ из нулей и единиц:

$$\omega_A^{f^{\sigma_0}(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})} = \omega_A^{f(x_1, \dots, x_n)}.$$

2.6. Если $\omega_A^f = 1$ для некоторого A , то $\|f\| = \frac{1}{2}$.

Это утверждение следует из того факта, что между наборами $(\alpha_1, \dots, \alpha_{i_1}, \dots, \alpha_{i_k}, \dots, \alpha_n)$ и $(\alpha_1, \dots, \bar{\alpha}_{i_1}, \dots, \bar{\alpha}_{i_k}, \dots, \alpha_n)$ существует взаимно-однозначное соответствие, и для всех таких наборов $f(\alpha_1, \dots, \alpha_{i_1}, \dots, \alpha_{i_k}, \dots, \alpha_n) \neq f(\alpha_1, \dots, \bar{\alpha}_{i_1}, \dots, \bar{\alpha}_{i_k}, \dots, \alpha_n)$.

3. Допустимые наборы.

Определение 5 [4]. Набор чисел $(\omega_1, \omega_2, \dots, \omega_n)$ называется допустимым, если существует булева функция $f(x_1, x_2, \dots, x_n)$ такая, что $\omega_i = \omega_i^f$ для $i = \overline{1, n}$.

$\tilde{\sigma}$ -набором назовем набор чисел $\tilde{\sigma} = (\sigma_0, \sigma_1, \dots, \sigma_n)$, где $\sigma_i \in \{0, 1\}$, $i = \overline{0, n}$. $\tilde{\sigma}$ -процедурой назовем применение $\tilde{\sigma}$ -набора к некоторой функции $f(x_1, x_2, \dots, x_n)$, в результате чего получается новая функция $f^{\sigma_0}(x_1^{\sigma_1}, x_2^{\sigma_2}, \dots, x_n^{\sigma_n})$. Множество всех функций $f^{\sigma_0}(x_1^{\sigma_1}, x_2^{\sigma_2}, \dots, x_n^{\sigma_n})$, где $\sigma_i \in \{0, 1\}$, $i = \overline{0, n}$, называется $\tilde{\sigma}$ -семейством функции $f(x_1, x_2, \dots, x_n)$. Если две функции принадлежат одному $\tilde{\sigma}$ -семейству, то они называются родственными.

Теорема. Существуют неродственные функции с одинаковыми допустимыми наборами.

Доказательство. Для доказательства достаточно привести пример двух неродственных функций с одинаковыми допустимыми наборами.

Таким примером может служить пара функций $f_1 = (x_1 x_2 \vee x_1 x_3 \vee x_2 x_3) \oplus (x_4 x_5 \vee x_4 x_6 \vee x_5 x_6)$ и $f_2 = x_1 x_2 \vee x_3 x_4 \vee x_5 x_6$, для которых $\omega_i^{f_1} = \omega_i^{f_2} = \frac{1}{2}$, $i = \overline{1, 6}$ и $\omega_{1,2,3}^{f_1} = 1$, $\omega_{1,2,3}^{f_2} = \frac{1}{2}$.

4. Выделение активной части схемы. Из теоремы, изложенной в §4 [5], следует, что для любой булевой функции $f(x_1, \dots, x_n)$ и любого числа $\varepsilon > 0$ существует число $\delta > 0$ такое, что если $\max_{1 \leq i \leq n} \omega_i^f < \delta$, то $\min \{\|f\|, \|\bar{f}\|\} < \varepsilon$. Этот результат является теоретическим обоснованием возможности выделения активной части схемы. Для булевой функции эти вопросы рассмотрены в работе [6], где содержится разработка алгоритма выделения активной части булевой функции. Это фактически является разработкой нового направления в теории аппроксимации в области теории булевых функций.

Поскольку одним из способов задания булевой функции является соответствующая комбинационная логическая схема с одним выходом, то, очевидно, задача выделения активной части булевой функции автоматически интерпретируется в области цифровых логических схем в виде выделения активной части схемы. Но поскольку среда описания булевой функции меняется (имеется в виду переход из описания с помощью формулы к описанию с помощью комбинационной схемы с одним выходом), то алгоритм выделения активной части функции при ее описании формулой серьезным образом подвергается изменению, когда мы переходим из формульного описания функции к схемному. Более того, в настоящее время схемы описываются с помощью специальных языков описания аппаратур (Verilog HDL, VHDL, Alex HDL [6-8]). В нашем случае предпочтительным

является использование языка Alex, так как он построен аксиоматическим принципом и в нем легко осуществить эквивалентные и иные преобразования схем и их частей [9].

Выделение активной части комбинационной схемы с одним выходом осуществляется поэтапно.

На первом этапе вычисляются активности входов схемы. Если данная схема реализует функцию $f(x_1, \dots, x_i, \dots, x_n)$ и требуется вычислить активность аргумента x_i (т.е. входы схемы с номером i), то следует многократно вычислить сумму

$$f(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \oplus f(\alpha_1, \dots, \bar{\alpha}_i, \dots, \alpha_n)$$

для случайных наборов $(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$ из нулей и единиц и приблизительно вычислить активность указанного i -го входа схемы следующей формулой:

$$\omega_i^f \approx m / N,$$

где N - число экспериментов, т.е. число наборов $(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$, для которых многократно вычисляется вышеуказанная сумма, а m - число случаев, когда указанная сумма принимает значение 1. Погрешность точности вычисления этой активности равна $n / \sqrt{N}$, где n - длина наборов $(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$ [10].

Вторым этапом является подбор наиболее активных входов схемы, которые должны быть сохранены как входы активной части схемы, а остальные входы, наиболее пассивные, замещаются нулями или единицами таким образом, чтобы активная часть являлась наилучшим приближением для основной схемы.

Третьим этапом является оценка точности приближения с помощью активной части. Точность регулируется увеличением или уменьшением числа наиболее активных входов. В первом случае точность увеличивается, а во втором случае - уменьшается.

В таблице приводятся результаты экспериментов выделения активных частей некоторых подсхем схемы c7552- bench [11].

Таблица

Номер выхода подсхемы	Длина записи под- схемы на языке Alex	Активность входа, начи- ная с δ	Число входов подсхемы	Число входов акт. части схемы	Длина записи активной части	Точность приближения (ε)
58	1176	0,0001	94	22	692	0,0001
58	1176	0,0002	94	27	478	0,00024
58	1176	0,0003	94	25	486	0,00042
58	1176	0,0004	94	24	538	0,00051
59	1381	0,0001	124	37	485	0,00025
59	1381	0,0002	124	30	1054	0,00201
59	1381	0,0003	124	24	401	0,070088
59	1381	0,0004	124	22	1032	0,04606
60	1381	0,0001	124	36	453	0,00024
60	1381	0,0002	124	32	437	0,0006
60	1381	0,0003	124	22	392	0,07101
60	1381	0,0004	124	20	381	0,148
61	1177	0,0001	94	30	422	0,0001
61	1177	0,0002	94	26	383	0,0002
61	1177	0,0003	94	25	379	0,00034
61	1177	0,0004	94	24	374	0,00048

СПИСОК ЛИТЕРАТУРЫ

1. **Бозоян Ш.Е., Егиазарян В.С.** О наилучшем приближении булевых функций // Вестник ГИУА. Серия «Моделирование, Оптимизация, Управление». - 2006.-Вып.9, том 2.-С. 34- 42.
2. **Read J.S.** A Class of Multiple Error Correcting Codes and the Decoding Scheme// IRE Trans. Prof. Group Inform. Theory.- 1954.- 4.- P.38-49.
3. **Бозоян Ш.Е.** Некоторые свойства булевых дифференциалов и активностей аргументов булевых функций // Проблемы передачи информации.-1978. - Т.14, №1.-С.77-88.
4. **Бозоян Ш.Е., Егиазарян В.С.** Простые и составные наборы активностей аргументов булевых функций // Годичная научная конференция РАУ.- 2006.- С. 85-89.
5. **Бозоян Ш.Е.** Некоторые свойства булевых дифференциалов и активностей аргументов булевых функций и вопросы построения надежных схем из ненадежных элементов // Изв. АН СССР. Техническая кибернетика.-1975.- 5.- С. 148-160.
6. **Palnitkar S.** Verilog HDL: A Guide to Digital Design and Synthesis. SunSoftPress. Prentice Hall, 1996.
7. **Маршнер Ф.Е.** VHDL для моделирования, синтеза и формальной верификации аппаратуры. - М., 1995. - С.1-13.
8. **Бозоян Ш.Е., Егиазарян В.С.** Язык Alex описания схем // Журнал «Программирование».-2007.-№ 4.-С.65-80.
9. **Кочаров Д.А.** Некоторые классы булевых функций // Высокие технологии, фундаментальные и прикладные исследования, образование.- 2007.-Т.9.- С.53-56,

10. **Бозоян Ш.Е., Егиазарян В.С.** Активная часть цифровых схем и её применение в области автоматизированного проектирования схем // Труды VI Международной конференции SICPRO`08.-М., 2008.-С.1205-1210.
11. **Hansen M., Yalcin H., Hayes J.P.** Unveiling the ISCAS-85 Benchmarks: A Case Study in Reverse Engineering // IEEE Design and Test. -1999.- Vol. 16, № 3. - P.72-80, July-September.

ГИУА. Материал поступил в редакцию 11.09.2007.

Շ.Ե. ԲՈԶՈՅԱՆ, Վ.Ս. ԵԴԻԱԶԱՐՅԱՆ, Դ.Ա. ԲՈՉԱՐՈՎ, Ն.Վ.ԲԱԴԱԼՅԱՆ

**ԲՈՒԼՅԱՆ ԴԻՖԵՐԵՆՑԻԱԼՆԵՐԻ ԵՎ ԲՈՒԼՅԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ
ԱՐԳՈՒՄԵՆՏՆԵՐԻ ԱԿՏԻՎՈՒԹՅՈՒՆՆԵՐԻ ԿԻՐԱՌՈՒԹՅՈՒՆԸ ՍԽԵՄԱՅԻ ԱԿՏԻՎ ՄԱՍԻ
ԱՆՋԱՏՄԱՆ ՀԱՄԱՐ**

Դիտարկվում են բուլյան դիֆերենցիալ, նրա հիմնական հատկությունները, բուլյան ֆունկցիայի փոփոխականների համախմբի ակտիվությունը, համակցված բուլյան ֆունկցիա իրականացնող մեկ էլք ունեցող համակցված սխեմա: Օգտագործելով համակցված սխեմայի մուտքերի ակտիվությունները և սխեմայի ակտիվ մասի կառուցման ալգորիթմը, անջատվում են թեստային էտալոնային սխեմաների (ISCAS-85) մեկ էլք ունեցող ենթասխեմաների ակտիվ մասերը:

Առանցքային բառեր. բուլյան դիֆերենցիալ, նախագծում, թվային սխեմա, ակտիվ մաս:

SH.E. BOZOYAN, V.S. YEGHIAZARYAN, D.A. KOCHAROV, N.V. BADALYAN

**BOOLEAN DIFFERENTIALS AND ACTIVITIES OF VARIABLE BOOLEAN
FUNCTIONS FOR SEPARATING ACTIVE PART OF CIRCUIT**

The Boolean differential and its main characteristics, the activity of variable Boolean function combination are examined. Combinational digital circuits are examined also with one output, realizing the Boolean function. Using activities of the combinational circuits inputs and the algorithm of building the active part of circuits for test standard circuits (ISCAS-85) the active parts of subcircuits having one output are allocated.

Keywords: Boolean differential, designing, digital circuits, active part.