УДК 656.25

АВТОКОРРЕЛЯЦИОННОЕ ТЕСТИРОВАНИЕ ЦИФРОВЫХ КОМБИНАЦИОННЫХ СХЕМ

Чернов А.В.[1], Сергеева Е.А.[2]

[1]ФГБОУ ВПО «Ростовский государственный строительный университет», Ростов-на-Дону, Россия (344022, Ростов-на-Дону, ул. Социалистическая, 162),e-mail: a.v.chernov@pmvt.ru
[2]ФГБОУ ВПО «Ростовский государственный университет путей сообщения», Ростов-на-Дону, Россия (344038, Ростов-на-Дону, пл. им. Ростовского Стрелкового полка Народного Ополчения, 2)

В статье предложен метод определения неисправностей типа «постоянный 0» и «постоянная 1» в цифровых комбинационных схемах. Подробно рассмотрен подход к тестированию цифровых комбинационных схем, основанный на вычислении тестового «синдрома» для логических функций. Обозначены преимущества и недостатки подхода, связанного с синдромным тестированием. Приведены необходимые математические выражения тестового синдрома, а также рекурсивная процедура его вычисления. Рассмотрено преобразование Уолша с матрицей Адамара для спектрального представления булевых функций. Показан пример расчета преобразования Уолша с матрицей Адамара для конкретной булевой функции. Указана связь между рассматриваемым спектральным преобразованием и тестовым синдромом. Приведено выражение расчета тестового синдрома по спектральному коэффициенту. Показан пример, позволяющий выявить недостатки тестового синдрома. Разработан метод составления тестовых векторов, использующий свойства автокорреляционной функции булевой функции. В автокорреляционном тестировании доказано утверждение, применимое для тестирования рассматриваемого класса неисправностей в цифровых комбинационных схемах.

Ключевые слова: булева функция, комбинационная схема, тестовый синдром, автокорреляционная функция булевой функции, автокорреляционное тестирование

AUTOCORRELATIONTESTINGOFDIGITALCOBMBINATIONALCIRCUITS

Chernov A.V.[1], Sergeeva E.A.[2]

[1] Rostov State Building University, Rostov-on-Don, Russia, (344022, Rostov-on-Don, street Sotsialisticheskaja, 162), e-mail: a.v.chernov@pmvt.ru
[2] Rostov State Transport University, Rostov-on-Don, Russia, (344038, Rostov-on-Don, square n.a.RostovskogoStrelkovogo polka NarodnogoOpolchenija, 2)

This paper proposes a method for determining the fault type "constant 0" and "constant 1" in digital combinational circuits. The approach to the testing of digital combinational circuits based on the calculation of the test syndrome for logic functions is detailed. Advantages and disadvantages of the approach associated with syndrome testing are marked. The necessary mathematical expressions test syndrome, as well as a recursive procedure of its calculation are considered. A Walsh transform with Hadamard matrix for the spectral representation of Boolean functions is determined. An example of calculation of Walsh transform with Hadamard matrix for a particular Boolean functionhas been done. The relation between the spectral transformation and test syndrome is detailed. An expression for the calculation of the test syndrome spectral coefficients is given. An example that allows the test to identify deficiencies syndromehas been done. A method of making the test vectors, using the properties of the autocorrelation function of a Boolean function is developed. In the autocorrelation test is proven the statement, applicable to test the class of faults in digital combinational circuits .

Keywords: Boolean function, combinational circuit, test syndrome, autocorrelation function of a Boolean function, autocorrelation test

Введение

Комбинационные схемы являются основой построения всех современных цифровых устройств обработки информации. Усложнение самих цифровых устройств, высокая степень их интеграции естественным образом усложняют задачи их тестирования и, конечно, полностью исключают переборные методы тестирования. Пути поиска компактных тестов

для цифровой аппаратуры без снижения полноты и глубины тестирования были обозначены достаточно давно. Одним их подходов компактному тестированию и синтезу цифровых схем [3], а также к исследованию булевых функций в области криптографии [8] является их представление в виде наборов спектральных коэффициентов преобразования Уолша (в общем виде Адамара-Радемахера-Уолша, так как используются различные матрицы для преобразования). Данное преобразование хорошо исследовано и для него разработаны различные алгоритмы быстрых преобразований [1]. Автором в работах [2,4] рассматривались спектральные преобразования Уолша для булевых функций, применительно к некоторым задачам технической диагностики. Отметим также, что в рамках данной статьи под тестированием понимается выявление лишь константных неисправностей вида «постоянный 0» и «постоянная 1».

Тестовый «синдром» и спектральное преобразование

Особенностью спектрального представления булевых функций является не только компактность самого теста, но и возможность непосредственного встраивания тестов в цифровое устройство для решения задач онлайновой диагностики и самодиагностики. Идея составления теста по спектральному преобразованию булевой функции восходит к работе [7], в которой предложен тестовый «синдром» (в дальнейшем без кавычек), назначением которого является различение логической функции, описывающей исправное устройство, от логической функции, измененной под воздействием возникшей в устройстве неисправности. В работе [7] тестовый синдром S определен для трех логических операций ($И$, $ИЛИ$, $\oplus$ – исключающее $ИЛИ$) как отношение числа минитермов K булевой функции, содержащей только одну операцию к 2^n, то есть $S = K / 2^n$, где n означает число входов функции. Таким образом, синдром является некоторым числом $0 \le S \le 1$, характеризующим функцию в зависимости от базиса её представления и рассчитывается для логических функций, содержащих только одну логическую операцию со значениями $x_i^* \in \{x_i, \overline{x}_i\}$, $i = 1, 2, ..., n$.:

1) для многовходового логического $И$ синдром $S\left(x_1^* x_2^* ... x_n^*\right) = 2^{-n}$ (1)

2) для многовходового логического $ИЛИ$ синдром $S\left(x_1^* + x_2^* + ... + x_n^*\right) = 1 - 2^{-n}$; (2)

3) для многовходового логического $\oplus$ – синдром $S\left(x_1 \oplus x_2 \oplus x_2 \oplus ... \oplus x_n\right) = 1/2$. (3)

Синдром S_{out}, получающийся в результате объединения двух синдромов S_1, S_2 разными операциями зависит от её вида:

1) $НЕ(S_1)$ рассчитывается $S_{out} = 1 - S_1$; (4)

2) S_1 $И$ S_2 рассчитывается $S_{out} = S_1 S_2$; (5)

3) S_1 $ИЛИ$ S_2 рассчитывается $S_{out} = S_1 + S_2 - S_1 S_2$; (6)

4) $S_1 \oplus S_2$ рассчитывается $S_{out} = S_1 + S_2 - 2S_1S_2$. (7)

Для всей комбинационной схемы, реализуемой функцией f, для тестирования входа x_i на изменение его значения на константу 0 или 1, существует её представление:

$$f = Ax_i + B\overline{x}_i + C,$$

где A, B, C – выражения, не зависящие от x_i,

а «синдром» $S(f) = \dfrac{S(A\overline{C}) + S(B\overline{C})}{2} + S(C)$. (8)

Процедура расчета комбинационной схемы с помощью представленного синдрома следующая. Начиная с представления схемы в виде булевой функции в дизъюнктивной нормальной форме рекурсивно применять формулы (1)-(8), исключая каждый раз по одной входной переменной. Такой расчет возможен в онлайновом режиме и не требует формирования и сохранения множества тестовых векторов, хотя требует дополнительных ячеек памяти и выходов комбинационной схемы. Также, такой синдром оказывается не применимым к некоторым видам схем. Для преодоления этих недостатков были предложены методы тестирования схем, использующие свойства спектральных преобразований булевых функций.

Спектральное преобразование булевой функции выполняется следующим образом. Зададим булеву функцию $f(x)$ в векторном виде $\mathbf{Y} = \left(f(0), f(1), ..., f\left(2^n - 1\right)\right)^{\mathrm{T}}$, где n – число входных значений. Преобразование Уолша в общем случае имеет вид

$$\mathbf{R} = \frac{1}{2^n}\mathbf{T}^n\mathbf{Y}, \quad (9)$$

где $\mathbf{T}^n$ – матрица размерности $2^n \times 2^n$, зависящая от вида выбираемого преобразования.

В данной статье выберем матрицу Адамара и приведем пример для конкретной булевой функции $f(x) = \overline{x}_1\overline{x}_2x_3 + \overline{x}_1x_2\overline{x}_3 + x_1\overline{x}_2\overline{x}_3 + x_1x_2x_3$. Выходной вектор $\mathbf{Y}$ функции $f(x)$ равен $\mathbf{Y}^{\mathrm{T}} = [0,1,1,0,1,0,0,1]$. Выполним n-точечное преобразование Уолша-Адамара $\mathbf{R} = \mathbf{HY}$ с матрицей Адамара $\mathbf{H}$:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -0.5 \end{bmatrix}.$$

$$\mathbf{H} \qquad \mathbf{Y} \qquad \mathbf{R}$$

В результате булева функция представлена вектором спектральных коэффициентов $\mathbf{R}^{\mathrm{T}} = [r_0, r_1, ..., r_7] = [0.5, 0, 0, 0, 0, 0, 0, -0.5]$.В работе [6] указана формула расчета синдромабулевой функции $f(x), x = \{x_1, x_2, ..., x_n\}$:

$$\sigma[f(x)] = \frac{1}{2^n} \sum_{v=0}^{2n-1} f(v), \tag{10}$$

где $f(v) = f(x)$, для $x_i = v_i,\ 1 \le i \le n,\ v = \sum_{j=1}^{n} v_j 2^{j-1}$.

Решение о неисправности схемы принимается из условия $\sigma(f) \neq \sigma(\hat{f})$, где f – функция исправной схемы, $\hat{f}$ – функция, измененная в результате неисправности. Также в [6], показано, что спектральный коэффициент r_0 преобразования Уолша $\mathbf{R} = \mathbf{HY}$ (без множителя $1/2^n$) связан с синдромом:

$$r_0 = 2^n \sigma[f(x)]. \tag{11}$$

Ранее было указано, что синдромное тестирование не применимо к некоторым видам комбинационных схем. Для иллюстрации возьмем приведенную выше в примере функцию $f(x) = \overline{x}_1\overline{x}_2x_3 + \overline{x}_1x_2\overline{x}_3 + x_1\overline{x}_2\overline{x}_3 + x_1x_2x_3$ и рассчитаем синдром. Выходной вектор $\mathbf{Y}^{\mathrm{T}} = [0,1,1,0,1,0,0,1]$, $\mathbf{R} = \mathbf{HY}$, $\mathbf{R}^{\mathrm{T}} = [r_0, r_1, ..., r_7] = [4,0,0,0,0,0,0,4]$ и по (11) $\sigma = 1/2$. Теперь положим, что в схеме есть константная неисправность $X_3 = 0$.Тогда $\hat{f}(x) = \overline{x}_1x_2 + x_1\overline{x}_3$, $\mathbf{Y}^{\mathrm{T}} = [0,1,1,0]$, $\mathbf{R} = \mathbf{HY} = [2,0,0,2]$, $r_0 = 2$, и по (11) $\sigma = 1/2$.Синдромы равны между собой $\sigma(f) = \sigma(\hat{f}) = 1/2$ и неисправность определить нельзя, поэтому необходимо усовершенствовать данный метод.

Автокорреляционное тестирование и основной результат

В приведенном выше примере, функция с внесением неисправности представляет собой функцию логического $\oplus$, которую вправе можно назвать одной из «трудно

тестируемых» функций. Для достижения тестируемости функций такого вида предлагается применение автокорреляционного тестирования с возможностью различения типа неисправности.

Автокорреляционная функция [5] $B(x)$ для n-аргументной булевой функции $f(x)$ определяется как

$$B(x)=\sum_{\tau=0}^{2^{n-1}} f(\tau)f(\tau\oplus x).$$

Выразим автокорреляционную функцию в терминах спектральных коэффициентов r_α и r_β, где $\alpha,\beta\in S=\{1,2,...,n\}$. Из преобразования Уолша-Адамара $\mathbf{F}=\frac{1}{2^n}\mathbf{HR}$, получаем

$$f(\tau)=\frac{1}{2^n}\sum_{\alpha=0}^{2^{n-1}}\mathbf{H}[\tau,\alpha]r_\alpha \text{ и } f(\tau\oplus x)=\frac{1}{2^n}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[\tau x,\beta]r_\beta.$$

Найдем значение выражения

$$f(\tau)\,f(\tau\oplus x)=\frac{1}{2^{2n}}\sum_{\alpha=0}^{2^{n-1}}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[\tau,\alpha]\mathbf{H}[\tau x,\beta]r_\alpha r_\beta=\frac{1}{2^{2n}}\sum_{\alpha=0}^{2^{n-1}}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[\tau,\alpha]\mathbf{H}[\tau,\beta]\mathbf{H}[x,\beta]r_\alpha r_\beta=$$

$$=\frac{1}{2^{2n}}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[x,\beta]r_\beta^2+\sum_{\alpha=0}^{2^{n-2}}\sum_{\beta=0,\beta\neq\alpha}^{2^{n-1}}\mathbf{H}[\tau,\alpha\beta]\mathbf{H}[x,\beta]r_\alpha r_\beta.$$

$$\sum_{\tau=0}^{2^{n-1}} f(\tau)f(\tau\oplus x)=\frac{1}{2^{2n}}\left[\sum_{\alpha=0}^{2^{n-1}}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[x,\beta]r_\beta^2+\sum_{\alpha=0}^{2^{n-2}}\sum_{\beta=0,\beta\neq\alpha}^{2^{n-1}}\sum_{\tau=0}^{2^{n-1}}\mathbf{H}[\tau,\alpha\beta]\mathbf{H}[x,\beta]r_\alpha r_\beta\right].$$

Тогда

$$B(x)=\sum_{\tau=0}^{2^{n-1}} f(\tau)f(\tau\oplus x)=\frac{1}{2^n}\sum_{\beta=0}^{2^{n-1}}\mathbf{H}[x,\beta]r_\beta^2=\frac{1}{2^n}\sum_{v=0}^{2^{n-1}}\mathbf{H}[x,v]r_v^2, \qquad (12)$$

где r_v $-v$-й спектральный коэффициент.

В автокорреляционном тестировании автокорреляционная функция исправной комбинационной схемы сравнивается с автокорреляционной функцией комбинационной схемы с неисправностью.

Докажем

У т в е р ж д е н и е

Неисправность типа «постоянный 0» либо «постоянная 1» обнаруживается, если для $x>1$, $i=\{1,...,n\}$, *для спектральных коэффициентов* r_v *исправной функции и спектральных коэффициентов функции с* i*-й неисправностью* r_{v_i}

$$\sum_{\tau=0}^{2^{n-1}}\mathbf{H}[x,\tau]\left(r_{v_i}^2\pm r_v r_{v_i}\right)\neq 0.\square$$

Д о к а з а т е л ь с т в о

Из выражения (12) следует, что для функции без неисправности автокорреляционная функция выражается

$$B(x)=\frac{1}{2^n}\left[\sum_{\tau=0}^{2^{n-1}}\mathbf{H}[x,\tau]r_v^2+\sum_{v_i=0}^{2^{n-1}}\mathbf{H}[x,v_i]r_{v_i}^2\right].$$

Для функции с неисправностью автокорреляционная функция будет

$$B^*(x)=\frac{1}{2^n}\left[\sum_{\tau=0}^{2^{n-1}}\mathbf{H}[x,\tau]\left(r_v^2+r_{v_i}^2\pm 2r_v r_{v_i}\right)\right].$$

Заметим, что из-за возникновения неисправности $\mathbf{H}[x,\tau]=-\mathbf{H}[x,v_i]$.Вычтем $B(x)-B*(x)$ и получаем

$$B(x)-B*(x)=-\frac{1}{2^n}\sum_{\tau=0}^{2^{n-1}}\mathbf{H}[x,\tau]\left(r_{v_i}^2\pm r_v r_{v_i}\right).\blacksquare$$

Рассмотрим пример: для булевой функции $f(x)=x_1\overline{x}_2+x_2\overline{x}_3+\overline{x}_1x_3+x_4x_5+\overline{x}_4\overline{x}_5$ автокорреляционные функции, предназначенные для тестирования неисправностей вида «константный 0» и «константная 1» будут

$$B(x_1)=x_1,\ B(x_2)=x_1\oplus x_2,B(x_3)=x_1\oplus x_3,\ B(x_4)=x_1\oplus x_4,B(x_5)=x_1\oplus x_5,$$

а в матричном виде тестовые вектора $T_{12345}=\begin{bmatrix}1&0&0&0&0\\1&1&0&0&0\\1&0&1&0&0\\1&0&0&1&0\\1&0&0&0&1\end{bmatrix}$.

Работа выполнена при финансовой поддержке РФФИ, проекты 13-01-00325-а, 13-01-00637-а.

Список литературы

1. Ахмед Н. Ортогональные преобразования при обработке цифровых сигналов / Ахмед Н., Рао К.Р.: Пер. с англ. –М.: Связь. – 1980. – 248с.

2. Гуда А.Н. Алгоритмы спектральных и символьных преобразований булевых функций для решения задач анализа и проектирования технологически безопасных информационных систем // Гуда А.Н., Чернов А.В. // Вестник Ростовского государственного университета путей сообщения. – 2008. – №2. – С. 46-53.

3. Карповский М.Г. Спектральные методы анализа и синтеза дискретных устройств. Библиотека по автоматике, выпуск 507 / Карповский М.Г., Москалев Э.С. – Л., «Энергия». – 1973. – 144 с.
4. Чернов А.В. Спектральные преобразования дискретных функций для вычисления логических производных / Чернов А.В., Калинин Т.С. // Обозрение прикладной и промышленной математики. – 2010. – Т.17, №6. – С. 1049-1051.
5. Aborhey S. Autocorrelation testing of combinational circuits / Aborhey S. // Computers and Digital Techniques, IEE Proceeding E. – 1989. – V. 136, issue 1. – PP. 57-61.
6. Eris E. Syndrome and autocorrelation-testable internally unate combinational networks / Eris E., Muzio J.C. // Electron. Lett. – 1984. –№20, (6). –PP. 264-266.
7. Savir J. Syndrome-testable design of combinational circuits / Savir J. // IEEE Trans. Com-put. – 1980. – C-29. – PP. 442-451.
8. Tarannikov Y., Autocorrelation coefficients and correlation immunity of Boolean functions / Korolev P., Botev A. // Advances in Cryptology ASIACRYPT – 2001, Lecture Notes in Computer Science 2248. – Springer-Verlag. – PP. 460-480.

Рецензенты:
Беляков С.Л., д.т.н., профессор кафедры информационно-аналитических систем безопасности Южного федерального университета, г. Таганрог.
Бутакова М.А., д.т.н., профессор кафедры информатики ФГБОУ ВПО Ростовский государственный университет путей сообщения, г. Ростов-на-Дону.