МИНИСТЕРСТВО ОБРАЗОВАНИЯ УКРАИНЫ
ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

РГАСНТИ 50.09 УДК 681.326.7

О.Н.Дяченко, И.А.Козицкий

ЗФФЕКТИВНОСТЬ КОМПАКТНОГО ТЕСТИРОВАНИЯ КОМБИНАЦИОННЫХ СХЕМ С ЛОКАЛИЗАЦИЕЙ ОШИБОК

Донецк 1996

В компьютерных системах контроля и диагностики средств вычислительной техники широкое применение находят устройства компактного анализа (УКА) выходных последовательностей, позволяющие значительно сократить объем информации, необходимой для проведения тестового эксперимента. В таких устройствах производится сжатие тестовой реакции объекта диагностики в компактную оценку. В зависимости от метода компактного анализа в качестве такой оценки может выступать контрольная сумма, синдром, сигнатура и т.д. В любом УКА возможна компенсация ошибок. Поэтому для любого метода компактного анализа актуальна задача определения достоверности результатов тестового эксперимента.

В большинстве работ, посвященных решению этой задачи, рассматриваются вопросы компенсации ошибок в анализаторах тестовых реакций (АТР) без учета генератора тестовых последовательностей (ГТП) и неисправностей в объекте диагностики. В результате получаются оценки достоверности, которые могут значительно отличаться от реальных.

Синдромное тестирование - один из первых подходов определения достоверности компактного тестирования с учетом конкретных неисправностей комбинационных схем (КС) [1]. Этот подход заключается в анализе тестируемости схемы на основе аналитического расчета компактных оценок по булевому выражению, которое описывает КС. Известны оценки достоверности на основе такого подхода в области сигнатурного анализа, в частности, для вариантов (псевдо-) исчерпывающего компактного тестирования при применении в качестве ГТП и АТР регистров сдвига с линейными обратными связями (РСЛОС) при условии, что образующие полиномы являются минимальными примитивными, либо РСЛОС АТР представляет собой произведение минимальных примитивных полиномов [2,3,4].

Данная работа посвящена оценке эффективности компактного тестирования КС при предположении, что ГТП - РСЛОС с примитивным образующим полиномом, а АТР реализованы на основе циклических кодов. Особенностью таких анализаторов является их способность локализовать ошибки, кратность которых не превышает корректорующих способностей кодов, на основе которых они построены.

Прежде всего рассмотрим метод аналитического расчета сигнатур, альтернативный методу, предложенному в [3].

Предположим, что ГТП и АТР реализованы в виде РСЛОС с внутренними сумматорами в цепях обратной связи с порождающими полиномами соответственно h(X) и g(X), причем оба полинома примитивные, а их корни связаны равенством $b=a^k$, m=degh(X)=degg(X).

Тестовые наборы, которые поступают на входы исследуемой КС, представляют собой ненулевые элементы поля $GF(2^m)$, являющегося расширением поля GF(2) над полиномом h(X). Эти элементы поля могут быть представлены в двоичном, полиномиальном и степенном обозначениях. Каждому ненулевому элементу a^k поля $GF(2^m)$ соответствует минимальный полином, причем, если минимальный полином примитивный, то его степень равна m. Если в качестве порождающего полинома РСЛОС АТР выбрать минимальный полином, соответствующий элементу a^k, то между корнями полиномов h(X) и g(X) будет выполнено равенство $b=a^k$. Анализ таблицы минимальных полиномов [5] показывает, что для любой степени m<5 существует только два примитивных полинома, причем $b=a^{-1}$, т. е. эти полиномы являются двойственными (взаимообратными). Поэтому для примеров, иллюстрирующих метод аналитического расчета сигнатур, будем рассматривать h(X) и g(X) степени m=5.

Основное отличие предлагаемого метода расчета сигнатур от известного [3] заключается в выборе степенного обозначения тестовых наборов вместо двоичного. В этом случае значение сигнатуры для конъюнкции с рангом m может быть вычислено согласно следующему выражению: $S=M_k X^{-Ak}$, где X^A - степенное обозначение тестового набора, M- матрица для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР.

Рассмотрим порядок расчета сигнатур на примерах.

Пример. Пусть $F_1=\bar{x}_5 \bar{x}_4 x_3 x_2 x_1$, $g(X)=X^5+X^3+1$, т.е. k=-1.

Элемент поля $GF(2^5)$ над полиномом $h(X)=X^5+X^2+1$, соответствующий тестовому набору 00111, может быть представлен в полиномиальном обозначении X^2+X+1. Для перехода к степенному обозначению воспользуемся таблицей логарифмов Зеча (табл. 1). Согласно этой таблице $X^j=X^i+1$. Учитывая свойства $X^{2j}=(X+1)^2$ и $X^i=(X^{p-i}+1)$, где $p=2^m-1$, определим таблицу для нечетных значений i от 1 до 15. Таким образом, $X^2+X+1=X(X+1)+1=XX^{18}+1=X^{19}+1=X^{11}$. Значение сигнатуры $S(F_1)=M_{-1}X^{11}$.

Таблица 1

Логарифмы Зеча для $h(X)=X^5+X^2+1$

i	1	3	5	7	9	11	13	15
j	18	29	2	22	16	19	14	24

Несколько замечаний по поводу построения матрицы M_k. Прежде всего следует отметить, что вид матрицы M_k зависит не только от k, но также от начального значения РСЛОС ГТП, которое может быть выбрано любым ненулевым. Каждому элементу поля a^0, a^1,..., a^{m-1} ставится в соответствие строка матрицы M_k, которая определяется следующим образом. Для элемента a^i отыскивается значение степени j эквивалентного элемента $a^j=a^i$, которое нацело делится на -k. Значение j определяется на основании равенства $a^i=a^{i+pd}$, где d- любое целое число. Строка матрицы M_k представляет собой остаток от деления полинома $X^{p+j/k+(s-1)}$ на полином g(X) (s - начальное состояние РСЛОС ГТП).

Для рассматриваемого примера при начальном состоянии РСЛОС ГТП, равном 00001, Матрица M_{-1} будет иметь вид:

$$M_{-1} = \begin{vmatrix} 01011 \\ 10110 \\ 00101 \\ 01010 \\ 10100 \end{vmatrix}$$

Для строки, соответствующей a^0, значение равно остатку от деления полинома $X^{31-0-1}=X^{30}$ на полином $g(X)=X^5+X^3+1$.

Для начального состояния РСЛОС ГТП равного a^0 и $k=-1$ матрица M_{-1} представляет собой последние m состояний РСЛОС АТР.

Для начального состояния РСЛОС ГТП равного a^m и $k=-1$ матрица M_{-1} представляет собой единичную матрицу, например, при m=5

$$M_{-1} = \begin{vmatrix} 00001 \\ 00010 \\ 00100 \\ 01000 \\ 10000 \end{vmatrix},$$

тогда значение сигнатуры конъюнкции с рангом m будет равно двоичному обозначению соответствующего элемента поля, записанному в обратном порядке.

Итак, $S(F_1)=M_{-1}X^{11}$. Для умножения на матрицу необходимо перейти от степенного обозначения тестового набора к двоичному (или полиномиальному). Такое преобразование можно упростить, используя заранее вычисленные значения X^1, X^2, X^4, X^8, X^{16} и т.д. по модулю h(X) (эффективность такого упрощения увеличивается с ростом значения m): $X^1 \bmod h(X)=X^1$, $X^2 \bmod h(X)=X^2$, $X^4 \bmod h(X)=X^4$, $X^8 \bmod h(X)=X^3+X^2+1$, $X^{16} \bmod h(X)=X^4+X^3+X+1$. Произвольный элемент X^i можно представить в виде произведения полиномов со степенями степени 2: $X^{11}=X^8X^2X^1$. Остаток от деления X^{11} на h(X) будет равен остатку от деления на h(X) произведения остатков сомножителей:

$(X^3+X^2+1)X^2X^1 \bmod h(X)=(X^6+X^5+X^3) \bmod (X^5+X^2+1)=X^2+X+1$, или в двоичном обозначении 00111.

При начальном значении РСЛОС ГТП a^5 значение сигнатуры $S(F_1)=11100$.

Пример. Пусть $F_2=\bar{x}_5\bar{x}_4x_3x_2$ при тех же значениях h(X),g(X) и том же начальном состоянии РСЛОС ГТП.

$$S(F_2)=M_{-1}(X^{19})^1+M_{-1}(X^{19}+1)=M_{-1}(X^{19}+X^{19}+1)=M_{-1}(00001)=10000.$$

Пусть $F_3=\bar{x}_5\bar{x}_4x_3x_1$, $F_4=\bar{x}_4x_3x_2x_1$, $F_5=\bar{x}_5\bar{x}_4x_3$.

$$S(F_3)=M_{-1}(X^5+X^5+X)=M_{-1}(X)=M_{-1}(00010)=01000.$$

$$S(F_4)=M_{-1}(X^{11}+X^{11}+X^4)=M_{-1}(X^4)=M_{-1}(10000)=00001.$$

$$S(F_5)=M_{-1}(X^2+X^2+1+X^2+X+X^2+X+1)=M_{-1}(0)=0.$$

Таким образом, в общем случае для k=-1 сигнатура конъюнкции с рангом r=m-1 равна произведению матрицы M_{-1} и X^i, где i- индекс отсутствующей переменной, уменьшенный на единицу; сигнатура конъюнкции с r<m-1 равна нулю [2].

Пример. Пусть $F_1=\bar{x}_5\bar{x}_4x_3x_2x_1$, $g(X)=X^5+X^3+X^2+X+1$, т.е. $k=-3$, начальное состояние РСЛОС ГТП- a^0, т.е. 00001.

Определим матрицу M_{-3}.

Строка M_{-3}, соответствующая элементу a^0, представляет собой остаток от деления полинома X^{30} на полином g(X): s=0, $X^{31-0/3+(0-1)}=X^{30}$.

Элементу a^1 соответствует полином X^9: $a^1=a^{1+31*2}=a^{63}$; $X^{31-63/3+(0-1)}=X^9$. Аналогично:
a^2 - X^{19}: $a^2=a^{2+31}=a^{33}$; $X^{31-33/3+(0-1)}=X^{19}$;
a^3 - X^{29}: $a^3=a^3$; $X^{31-3/3+(0-1)}=X^{29}$;
a^4 - X^8: $a^4=a^{4+31*2}=a^{66}$; $X^{31-66/3+(0-1)}=X^8$.

Каждая степень полинома X^i отличается от степени предыдущего полинома на константу, в данном случае на 10: $X^{30-31}=X^{-1}$; $X^{-1+10}=X^9$; $X^{9+10}=X^{19}$; $X^{19+10}=X^{29}$; $X^{29+10-31}=X^8$. Поэтому все значения степеней можно вычислить по известным двум значениям степеней полиномов, соответствующих элементам a^0 и a^1. Аналогично можно поступать для произвольного k.

Матрица M_{-3} будет иметь следующий вид :

$$M_{-3}=\left|\begin{array}{c}01001\\11100\\11010\\10010\\10111\end{array}\right|$$

$$S(F_1)=M_{-3}(X^{11})^3=M_{-3}X^{33}=M_{-3}X^2=\left|\begin{array}{c}01001\\11100\\11010\\10010\\10111\end{array}\right|(00100)=11010.$$

Рассмотрим общий случай расчета значений сигнатур для произвольных примитивных полиномов h(X) и g(X) степени m, корни которых связаны равенством $b=a^{-3}$.

Для конъюнкции с рангом r=m $S=M_{-3}X^{3A}$, где A- степень элемента поля, двоичное представление которого совпадает с двоичным числом, полученным в результате замены в булевом выражении переменных с инверсией - нулями, переменных без инверсии - единицами, отсутствующих переменных (для общего случая) - нулями.

Для конъюнкции с рангом r=m-1 с отсутствующей переменной:

x_1 - $S=M_{-3}(X^A)^3+M_{-3}(X^A+1)^3=M_{-3}[(x^A)^3+(X^A+1)^3]=M_{-3}(X^{2A}+X^A+1)$;

x_2 - $S=M_{-3}(X^{2A+1}+X^{A+1}+X^3)$; x_3 - $S=M_{-3}(X^{2A+2}+X^{A+4}+X^6)$;

x_4 - $S=M_{-3}(X^{2A+3}+X^{A+6}+X^9)$ и т.д.

Для конъюнкции с рангом r=m-2 с отсутствующими переменными:

x_2,x_1 - $S=M_{-3}(X^{3A}+(X^A+1)^3+(X^A+X)^3+(X^A+X+1)^3)=M_{-3}(X^2+X)$;

x_3,x_1 - $S=M_{-3}(X^4+X^2)$; x_4,x_1 - $S=M_{-3}(X^6+X^3)$; x_5,x_1 - $S=M_{-3}(X^8+X^4)$;

x_3,x_2 - $S=M_{-3}(X^5+X^4)$; x_4,x_2 - $S=M_{-3}(X^7+X^5)$ и т.д.

Для конъюнкции с рангом r<m-3 $S=M_{-3}(0)=0$.

Таким образом, двум различным конъюнкциям с рангом r=m-2, у которых отсутствуют одинаковые переменные, соответствуют одинаковые сигнатуры независимо от степени h(X) и g(X). Для любой конъюнкции с рангом r<m-3 соответствующая ей сигнатура равна 0.

В [3,4] рассматривается пример определения сигнатуры для конъюнкции $F=\bar{x}_5\bar{x}_4x_2$: $S(F)=\frac{d}{dz_1}\frac{d}{dz_2}M^3(0,0,z_2,1,z_1)=$

$=M\frac{d}{dz_1}\frac{d}{dz_2}(z_2z_1;1+z_2;z_2+z;z_1;z_1)=M(10100)$.

Согласно предлагаемому методу расчета сигнатур

$S(F)=M(X^4+X^2)=M(10100)$.

Рассмотрим общий случай расчета значений сигнатур для произвольных примитивных полиномов h(X) и g(X) степени m, корни которых связаны равенством $b=a^{-5}$.

Для конъюнкции с рангом r=m $S=M_{-5}X^{5A}$.

Для конъюнкции с рангом r=m-1 с отсутствующей переменной:

x_1 - $S=M_{-5}(X^A)^5+M_{-5}(X^A+1)^5=M_{-5}[(x^A)^5+(X^A+1)^5]=M_{-5}(X^{4A}+X^A+1)$;

x_2 - $S=M_{-5}(X^{4A+1}+X^{A+4}+X^5)$; x_3 - $S=M_{-5}(X^{4A+2}+X^{A+8}+X^{10})$;

x_4 – $S=M_{-5}(X^{4A+3}+X^{A+12}+X^{15})$ и т.д.

Для конъюнкции с рангом r=m-2 с отсутствующими переменными:

x_2,x_1 – $S=M_{-5}(X^{5A}+(X^A+1)^5+(X^A+X)^5+(X^A+X+1)^5)=M_{-5}(X^4+X)$;

x_3,x_1 – $S=M_{-5}(X^8+X^2)$; x_4,x_1 – $S=M_{-5}(X^{12}+X^3)$ и т.д.

Для конъюнкции с рангом r<m-3 $S=M_{-5}(0)=0$.

После выполнения аналогичных операций получаем, что сигнатура равна нулю в следующих случаях: k=-7, r<m-4; k=-9, r<m-3; k=- 11, r<m-4; k=-13, r<m-4; для произвольного k r<m-1-w, где w- вес двоичной записи -k.

Если рассматривать полученный результат при конкретных значениях m, условие равенства сигнатуры нулю можно сформулировать иначе: $r<W[(k)_o]$, где $W[(k)_o]$- вес двоичной записи k в обратном коде.

Таким образом, если неисправность в КС, описываемой функцией F, приводит к тестовой реакции $F_н$, и в представлении $F+F_н$ в виде полинома Жегалкина присутствуют только конъюнкции с рангом $r<W[(k)_o]$, то $S(F+F_н)=S(F)+S(F_н)=0$, или $S(F)=S(F_н)$, т.е. неисправность будет необнаруженной [4].

Например, если для РСЛОС ГТП и АТР выбраны взаимообратные полиномы ($b=a^{-1}$) степени m, а проверяемая КС описывается булевой функцией от n<m-2 переменных, то ни одна неисправность в КС не будет обнаружена (за исключением неисправностей, преобразующих КС в последовательностную схему). Тот же самый результат получится в случае $b=a^{-3}$ и n<m-3 и т.д. Наилучший результат с точки зрения необходимого условия сигнатурной тестируемости получается при выборе одинаковых полиномов РСЛОС ГТП и АТР [4].

Итак, число w (вес двоичной записи -k) представляет собой параметр, с помощью которого можно оценить эффективность сигнатурного анализа при применении в качестве ГТП и АТР РСЛОС с порождающими примитивными полиномами одинаковой степени. Параметр w принимает минимальное значение 1 при k=-1, и максимальное значение m-1 при k=1.

Этот вывод также справедлив для многовходовых АТР и РСЛОС ГТП и АТР с альтернативной реализацией (с внешними сумматорами в цепях обратной связи).

До сих пор мы рассматривали полиномы h(X) и g(X), которые являются примитивными. Предположим, что g(X)- непримитивный минимальный порождающий полином РСЛОС АТР, $b=a^k$, degh(X)=m.

В этом случае в соответствии с изложенным ранее методом аналитического расчета получить значение сигнатуры для конъюнкции с рангом m нельзя, поскольку нельзя построить матрицу M_{-k}.

Например, пусть m=4, $h(X)=X^4+X+1$, $g(X)=X^4+X^3+X^2+X+1$, $b=a^3$. Для построения матрицы M_{-3} прежде всего необходимо найти для элементов a^i, $i=\overline{0,3}$, значение степени j эквивалентного элемента $a^j=a^i$, которое делится на число -3 без остатка. В данном случае показатель полинома $h(X)$ равен $2^m-1=15$, т.е. числу, кратному -3. Поэтому $j=i+15d$, где d- любое целое число, для $i=1,2$ нацело на -3 не делится. Таким образом, алгоритм построения матрицы M_{-k} для непримитивного полинома $g(X)$ неприменим.

В связи с этим рассмотрим следующую модель организации компактного тестирования КС. В таблице 2 представлены элементы поля $GF(2^4)$, построенного как расширение поля GF(2) над полиномом $h(X)=X^4+X+1$. Каждому ненулевому элементу a^i поля $GF(2^4)$, представляющему в двоичном виде тестовый набор ГТП, поставим в соответствие элемент поля a^{3i}. Предположим, что элементы поля a^{3i} в двоичном виде соответствуют значениям сигнатур конъюнкций

Таблица 2

Элементы поля $GF(2^4)$

В виде степени	В двоичном виде	В виде степени	В двоичном виде
0	0000		
a^0	0001	a^0	0001
a^1	0010	a^3	1000
a^2	0100	a^6	1100
a^3	1000	a^9	1010
a^4	0011	a^{12}	1111
a^5	0110	a^0	0001
a^6	1100	a^3	1000
a^7	1011	a^6	1100
a^8	0101	a^9	1010
a^9	1010	a^{12}	1111
a^{10}	0111	a^0	0001
a^{11}	1110	a^3	1000
a^{12}	1111	a^6	1100
a^{13}	1101	a^9	1010
a^{14}	1001	a^{12}	1111

с рангом m. Такие значения сигнатур получатся при следующих условиях: 1) тестовые наборы поступают на входы КС в обратном порядке от a^{14} до a^{0} (такую тестовую последовательность можно получить при применении РСЛОС ГТП с полиномом, двойственным h(X), $h'(X)=X^4+X^3+1$, и начальном состоянии РСЛОС ГТП, равном a^4 (для поля, построенного над полиномом h'(X))); 2) в качестве АТР используется РСЛОС с полиномом $h(X)=X^4+X+1$, на тактовый вход которого поступает утроенная тактовая частота синхроимпульсов по сравнению с тактовой частотой для РСЛОС ГТП, причем на информационный вход АТР поступает тестовая реакция на каждом третьем такте. Для рассматриваемой модели организации компактного тестирования значение сигнатуры для конъюнкции с рангом m может быть определено согласно выражению $S=X^{3A}$, где X^{A} - степенное представление элемента поля, соответствующего тестовому набору, на котором булева функция принимает единичное значение.

В данном случае нет необходимости в определении матрицы М. Для преобразования значения сигнатуры, представленной в степенном обозначении к двоичному виду, может быть использован алгоритм, изложенный ранее. Вместе с тем для анализа сигнатурной тестируемости КС достаточно знать сигнатуру в степенном представлении.

Расчет значений сигнатур для конъюнкций с рангом r<m ничем не отличается от рассмотренного ранее расчета для РСЛОС ГТП и АТР с примитивными минимальными полиномами, за исключением того, что в данном случае отсутствует матрица для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР. Поэтому результат, заключающийся в том, что сигнатура конъюнкции с рангом r<m-1-w, где w- вес двоичной записи числа -k, распространяется и для данного варианта реализации тестирования КС. Учитывая, что между сигнатурами в рассматриваемой модели организации компактного тестирования и при тестировании с РСЛОС ГТП и АТР, для которых h(X)- примитивный, g(X)- непримитивный, можно поставить взаимнооднозначное соответствие, этот результат справедлив для всех сочетаний h(X) и g(X), для которых h(X)- примитивный, g(X)- неприводимый.

Учитывая, что структура РСЛОС с приводимым образующим полиномом, который представляет собой произведение различных неприводимых полиномов, эквивалентна совокупности структур РСЛОС с неприводимыми полиномами- сомножителями, получаются следующие выводы. Максимальная эффективность компактного тестирования КС достигается для следующих вариантов:

1) АТР на основе кодов Хэмминга (локализация одиночных ошибок)- одинаковые образующие полиномы РСЛОС ГТП и АТР;

2) АТР на основе кодов БЧХ (локализация кратных независимых ошибок) - первый сомножитель образующего полинома РСЛОС АТР (минимальный полином, соответствующий элементу поля Галуа с наименьшей степенью j) должен быть равен примитивному образующему полиному РСЛОС ГТП. Остальные сомножители - минимальные полиномы, соответствующие элементам поля Галуа со степенями j+2, j+4 и т.д.

3) многовходовый АТР на основе кодов Бартона (локализация одиночного ошибочного вектора) - сомножитель образующего полинома РСЛОС АТР, соответствующий неприводимому полиному, должен быть равен примитивному образующему полиному РСЛОС ГТП;

4) многовходовый АТР на основе кодов Рида-Соломона, исправляющего одиночные ошибки (локализация одиночного ошибочного вектора)- корень первого сомножителя образующего полинома РСЛОС АТР должен быть равен корню примитивного образующего полинома РСЛОС ГТП;

5) многовходовый АТР на основе кодов Рида-Соломона, исправляющего ошибки кратности t (локализация t ошибочных векторов)- корень первого сомножителя образующего полинома РСЛОС АТР (эле-

мент поля Галуа со степенью j) должен быть равен корню примитивного образующего полинома РСЛОС ГТП; корни остальных полиномов-сомножителей - элементы поля Галуа со степенями j+1, j+2, j+3 и т.д.

Все варианты допускают аналитический расчет значений сигнатур.

В заключение отметим, что полученные результаты могут найти применение при реализации устройств компактного анализа либо в виде составной части внешнего тестового оборудования, либо для встроенного самотестирования средств вычислительной техники.

Литература

1. Savir J. Syndrome- testable design of combihational circuits// IEEE Trans. Comput. - 1980.- N 6.-P.442-451.
2. Ярмолик В.Н. Аналитический метод вычисления сигна тур для сетевых дискретных структур// Автоматика и вычисл. техника.- 1987.- N 5.- С.77-81.
3. Ярмолик В.Н., Калоша Е.П. Метод аналитического расчета сигнатур в диагностике// Электрон. моделирование.- 1989.- 11,N6. - С.50-54.
4. Ярмолик В.Н., Калоша Е.П. Эффективность сигнатурного анализа в самотестирующихся СБИС // Электрон. моделирование.- 1992.- 14,N3. - С.51-56.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976.- 594с., ил.