МЕТОД АНАЛИТИЧЕСКОГО ВЫЧИСЛЕНИЯ СИГНАТУР

Дяченко О.Н.

Методы компактного тестирования нашли широкое применение как для встроенных средств тестового диагностирования, так и для внешнего тестового оборудования. Достоинством этих методов является значительное сокращение объема информации, необходимой для проведения тестового эксперимента. Применение компактного тестирования предполагает наличие эталонных сигнатур. Для комбинационных схем (КС) существует три основных способа их получения: снятие сигнатур на заведомо исправной КС; вычисление сигнатуры путем моделирования КС; аналитический расчет значения сигнатуры на основе булевой функции, описывающей КС. Третий способ получения сигнатур предполагает исчерпывающее или псевдоисчерпывающее тестирование КС при некоторых известных структурах генераторов тестовых последовательностей (ГТП) и анализаторов тестовых реакций (АТР). Достоинством этого способа является не только то, что он позволяет получить сигнатуры на этапе проектирования КС, но также возможность определения на его основе достоверности результатов тестового эксперимента.

В [1] предложен метод аналитического расчета значений сигнатур для псевдоисчерпывающего тестирования КС при применении в качестве ГТП и АТР регистров сдвига с линейными обратными связями (РСЛОС) с взаимообратными примитивными порождающими полиномами; в [2] этот метод обобщен для случая примитивных порождающих полиномов, корни которых связаны равенством $b=a^k$. В данной работе предлагается метод аналитического расчета сигнатур, альтернативный методу, рассмотренному в [2].

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). Если m равно количеству переменных, от которых зависит булева функция, описывающая КС, то тестирование является псевдоисчерпывающим; если m больше - тестирование исчерпывающее.

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 [4] 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.

В таблице 1 приведены представления элементов поля $GF(2^5)$ над полиномом $h(X)=X^5+X^2+1$ в степенном, полиномиальном и двоичном обозначениях. Поскольку h(X) примитивен, то символы a в степенном обозначении можно заменить символом X.

Основное отличие предлагаемого метода расчета сигнатур от известного [2] 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_k- матрица для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР.

Рассмотрим порядок расчета сигнатур на примерах.

Пример. Пусть $F_1 = \overline{x_5}\,\overline{x_4}\,x_3\,x_2\,x_1$, $g(X)=X^5+X^3+1$, т.е. k=-1.

Элемент поля $GF(2^5)$ над полиномом $h(X)=X^5+X^2+1$, соответствующий тестовому набору 00111, мохет быть представлен в полиномиальном обозначении X^2+X+1. Для перехода к степенному обозначению воспользуемся таблицей логарифмов Зеча (табл. 2). Согласно этой таблице $X^j=X^i+1$. Учитывая свойства $X^{2j}=(X^i+1)^2$ 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 $S(F_1)=M_{-1}X^{11}$.

Несколько замечаний по поводу построения матрицы M_k . К сожалению, в [2,3] не рассматривается порядок построения такой матрицы. 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 (в [2,3] имеет место ограничение на начальное значение РСЛОС ГТП: 00...010). 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) (a^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 $g(X)=X^5 +X^3 +1$ (см. табл. 3).

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): $X^1 \text{ modh}(X)=X^1$, $X^2 \text{ modh}(X)=X^2$, $X^4 \text{ modh}(X)=X^4$, $X^8 \text{ modh}(X)=X^3 +X^2 +1$, $X^{16} \text{ modh}(X)=X^4 +X^3 +X+1$. Произвольный элемент X^i можно представить в виде произведения полиномов со степенями степени 2: $X^{11} =X^8 X^2 X^1$. Остаток от деления X^{11} на h(X) будет равен остатку от деления на h(X) произведения остатков сомножителей: $(X^3 +X^2 +1)X^2 X^1 \text{ modh}(X)=(X^6 +X^5 +X^3)\text{mod}(X^5 +X^2 +1)=X^2 +X+1$, или в двоичном обозначении 00111.

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

Пример. Пусть $F_2 = \overline{x_5}\ \overline{x_4}\ x_3\ x_2$ 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 $F_3 = \overline{x_5}\ \overline{x_4}\ x_3\ x_1$, $F_4 = x_4\ \overline{x_3}\ x_2\ x_1$, $F_2 = x_5\ \overline{x_4}\ \overline{x_3}$.

$S(F_3)=M_{-1} (X^5 +X^5 +X)=M_{-1} (X)=M_{-1}$ (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 [4].

Пример. Пусть $F_1 = \overline{x_5}\ \overline{x_4}\ x_3\ x_2\ x_1$, $g(X)=X^5+X^3+X^2+X+1$, 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 (см. табл.3):

$$M_{-3}=\begin{vmatrix} 01001 \\ 11100 \\ 11010 \\ 10010 \\ 10111 \end{vmatrix}$$

$S(F_1)=M_{-3}(X^{11})^3=M_{-3}X^{33}=M_{-3}X^2=M_{-3}(00100)=11010.$

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-2 $S=M_{-3}(0)=0$.

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-2 соответствующая ей сигнатура равна 0.

В [2,3] рассматривается пример определения сигнатуры для конъюнкции $F=\overline{x_5}\ \overline{x_4}\ x_2$: $S(F)=(d/dz_1)(d/dz_2)\,M(0,0,z_2,1,z_1)^3=$

$=M(d/dz_1)(d/dz_2)(z_2\,z_1;\ 1+z_2;\ z_2+z_1;\ z_1;\ z_1)=M(10100)$.

Согласно предлагаемому методу расчета сигнатур

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

Следует отметить, что при прежних условиях для m=6,7,8,... значения сигнатур будут равны произведению соответствующих матриц на (010100), (0010100), (00010100),...

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-2 $S=M_{-5}(0)=0$.

После выполнения аналогичных операций получаем, что сигнатура равна нулю в следующих случаях: k=-7, r<m-3; k=-9, r<m-2; k=-11, r<m-3; k=-13, r<m-3; для произвольного k r<m-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, несмотря на трудоемкость, а в некоторых случаях бессмысленность операций (например, для $b=a^{-1}$), предлагаемый метод аналитического расчета значений сигнатур позволяет сформулировать

важный вывод: при любом начальном состоянии РСЛОС ГТП и РСЛОС ГТП и АТР с порождающими примитивными полиномами, корни которых связаны равенством $b=a^k$, m=degh(X)=degg(X), значение сигнатуры конъюнкции с рангом r<m-

-w, где w - вес двоичной записи -k, равна нулю.

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

Полученный вывод позволяет распространить оценку эффективности сигнатурного анализа, полученную в [3], для произвольного начального значения РСЛОС ГТП: 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 [3].

Например, если для РСЛОС ГТП и АТР выбраны взаимообратные полиномы ($b=a^{-1}$) степени m, а проверяемая КС описывается булевой функцией от n<m-1 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-2 и т.д. Наилучший результат с точки зрения необходимого условия сигнатурной тестируемости получается при выборе одинаковых полиномов РСЛОС ГТП и АТР [3].

Таким образом, 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.

Литература

1. Ярмолик В.Н. Аналитический метод вычисления сигнатур для сете-вых дискретных структур// Автоматика и вычисл. техника.- 1987.- N5.- С.77-81.

2. Ярмолик В.Н., Калоша Е.П. Метод аналитического расчета сигна-тур в диагностике// Электрон. моделирование.- 1989.- 11,N6. -С.50-54.

3. Ярмолик В.Н., Калоша Е.П. Эффективность сигнатурного анализа в самотестирующихся СБИС // Электрон. моделирование.- 1992.- 14,N3.- С.51-56.

4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976.- 594с., ил.

Таблица 1 - Представления поля $GF(2^5)$

В виде степени	В виде полинома	В 2-ом виде
0	0	00000
a^0	1	00001
a^1	X	00010
a^2	X^2	00100
a^3	X^3	01000
a^4	X^4	10000
a^5	X^2+1	00101
a^6	X^3+X	01010
a^7	X^4+X^2	10100
a^8	X^3+X^2+1	01101
a^9	X^4+X^3+X	11010
a^{10}	X^4+1	10001
a^{11}	X^2+X+1	00111
a^{12}	X^3+X^2+X	01110
a^{13}	$X^4+X^3+X^2$	11100
a^{14}	$X^4+X^3+X^2+1$	11101
a^{15}	$X^4+X^3+X^2+X+1$	11111
a^{16}	X^4+X^3+X+1	11011
a^{17}	X^4+X+1	10011
a^{18}	$X+1$	00011
a^{19}	X^2+X	00110
a^{20}	X^3+X^2	01100
a^{21}	X^4+X^3	11000
a^{22}	X^4+X^2+1	10101
a^{23}	X^3+X^2+X+1	01111
a^{24}	$X^4+X^3+X^2+X$	11110
a^{25}	X^4+X^3+1	11001
a^{26}	X^4+X^2+X+1	10111
a^{27}	X^3+X+1	01011
a^{28}	X^4+X^2+X	10110
a^{29}	X^3+1	01001
a^{30}	X^4+X	10010

Таблица 3 - Состояния АТР

X^5+X^3+1	$X^5+X^3+X^2++X+1$
00001	00001
00010	00010
00100	00100
01000	01000
10000	10000
01001	01111
10010	11110
01101	10011
11010	01001
11101	10010
10011	01011
01111	10110
11110	00011
10101	00110
00011	01100
00110	11000
01100	11111
11000	10001
11001	01101
11011	11010
11111	11011
10111	11001
00111	11101
01110	10101
11100	00101
10001	01010
01011	10100
10110	00111
00101	01110
01010	11100
10100	10111

Таблица 2 - 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