ЭФФЕКТИВНОСТЬ ПСЕВДОИСЧЕРПЫВАЮЩЕГО ТЕСТИРОВАНИЯ КОМБИНАЦИОННЫХ СХЕМ

Дяченко О.Н.
Кафедра ЭВМ ДонГТУ
do@cs.dgtu.donetsk.ua

Abstract

Dyachenko O.N. Effectiveness of the pseudoexhaustive testing of the combinational circuits. *The method of analytical determination for compact estimations in case of using signature analyzers structures according to minimal polynomial is considered. A simple estimations of the efficiency for generators and analyzers based on linear shift feedback registers of different capacity are proved. The obtained results may be of use to self-testig circuit design, compact testing combinational circuits, built-in testing of digital circuits.*

Введение

Сложность построения тестов для современных БИС и СБИС привела к появлению целого ряда подходов и методов контролепригодного проектирования цифровых устройств. Метод сквозного сдвигового регистра за счет декомпозиции схемы на последовательностную и комбинационную части позволяет свести задачу тестирования сложного цифрового устройства к проверке сдвиговых регистров и комбинационных подсхем. С помощью незначительных аппаратных затрат сдвиговые регистры легко преобразуются в линейные переключательные схемы. В результате получаются самотестирующиеся схемы, в которых реализуется компактное тестирование комбинационных схем (КС). При этом линейные переключательные схемы выполняют роль генераторов тестовой последовательности (ГТП) и анализаторов тестовой реакции (АТР).

Применение компактного тестирования ставит задачу определения достоверности результатов тестового эксперимента. В [1,2,3,4,5] проведен анализ эффективности сигнатурного анализа при использовании в качестве ГТП и АТР регистров сдвига с линейными обратными связями (РСЛОС) с примитивными порождающими полиномами одинаковой степени.

Данная работа посвящена обобщению известных результатов на случай РСЛОС ГТП и АТР с порождающими полиномами кратной степени.

1. Аналитический расчет сигнатур для непримитивных неприводимых порождающих полиномов РСЛОС АТР

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 соотношением $b=a^k$, 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. В этом случае значение сигнатуры для конъюнкции с рангом m может быть вычислено согласно следующему выражению [4]: $S = M_k X^{-Ak}$, где X^A - степенное обозначение тестового набора, M_k - ьатрица для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР.

Рассмотрим случай, когда g(X) - непримитивный неприводимый полином, deg g(X)=m, при прежних остальных условиях. В соответствии с изложенным в [4] алгоритмом построения матрицы M_k получаем противоречие. Например, пусть m=4,

$h(X)=X^4 + X^3 +1$, $g(X)=X^4 +X^3 +X^2 +X +1$, $b=a^{-3}$. Для построения матрицы M_{-3} прежде всего необходимо найти для элементов a^i, i=0,3, значения степеней j эквивалентных элементов $a^j = a^i$, которые делятся на число 3 без остатка. Однако 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. Вместе с тем матрица M_{-3} может быть получена иным способом, который рассмотрим на примере.

Полином $g(X)=X^4 +X^3 +X^2 +X +1$ является неприводимым, degg(X)=4, поэтому можно построить поле $GF(2^4)$ над полиномом g(X) путем возведения в степень примитивного элемента. Примитивным элементом такого поля является элемент (a+1), а минимальным полиномом, соответствующим элементу (a+1), является примитивный полином : $[(X+1)^4 +(X+1)^3 +1] \bmod g(X)=0$. В таблице 1 представлены элементы поля GF(16) над полиномом g(X) в степенном и двоичном обозначениях; состояния РСЛОС ГТП (ненулевые элементы поля GF(16) над полиномом $h(X)= X^4 +X^3 +1$); значения сигнатур S_1 и S_0 для каждой конъюнкции с рангом m при начальных состояниях РСЛОС ГТП 0010, т.е. a^1 , и 0001, т.е. a^0 , соответственно.

Таблица 1

GF(16) над g(X)		РСЛОС ГТП		S_1	S_0
0	0000				
$(a+1)^0$	0001	a^0	0001	0001	1111
$(a+1)^1$	0011	a^1	0010	1111	1000
$(a+1)^2$	0101	a^2	0100	1000	0100
$(a+1)^3$	1111	a^3	1000	0100	0010
$(a+1)^4$	1110	a^4	1001	0010	0001
$(a+1)^5$	1101	a^5	1011	0001	1111
$(a+1)^6$	1000	a^6	1111	1111	1000
$(a+1)^7$	0111	a^7	0111	1000	0100
$(a+1)^8$	1001	a^8	1110	0100	0010
$(a+1)^9$	0100	a^9	0101	0010	0001
$(a+1)^{10}$	1100	a^{10}	1010	0001	1111
$(a+1)^{11}$	1011	a^{11}	1101	1111	1000
$(a+1)^{12}$	0010	a^{12}	0011	1000	0100
$(a+1)^{13}$	0110	a^{13}	0110	0100	0010
$(a+1)^{14}$	1010	a^{14}	1100	0010	0001

Значение S для конъюнкции с рангом 4 равно $S = M_{-3} X^{3A}$, где X^A - степенное обозначение тестового набора,

$$M = \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{matrix}$$, или $$M = \begin{matrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{matrix}$$

в зависимости от начального значения РСЛОС ГТП a^1 или a^0 соответственно.

Пусть $h(X)=X^4 +X+1$, т.е. $b=a^3$. Полином $X^4 +X+1$ является минимальным полиномом элемента $(a+1)^{14} =(a+1)^{-1}$ поля GF(16) над полиномом g(X): $[(X^3 +X)^4 +(X^3 +X) +1] \bmod g(X)=0$. Таблица 2 аналогична таблице 1. В данном случае состояния РСЛОС ГТП представляют собой ненулевые элементы поля GF(16) над полиномом $h(X)= X^4 +X+1$.

Значение S для конъюнкции с рангом 4 равно $S = M_{-3} X^{-3A} = M_{-3} X^{12A}$, поскольку 15-3=12 , где X^A - степенное обозначение тестового набора,

$$M = \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$, или $$M = \begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$$

в зависимости от начального значения РСЛОС ГТП a^1 или a^0 соответственно.

Таблица 2

GF(16) над	g(X)	РСЛОС ГТП		S_1	S_0
0	0000				
$(a+1)^0$	0001	a^0	0001	0001	1111
$(a+1)^1$	0011	a^1	0010	1111	1000
$(a+1)^2$	0101	a^2	0100	1000	0100
$(a+1)^3$	1111	a^3	1000	0100	0010
$(a+1)^4$	1110	a^4	0011	0010	0001
$(a+1)^5$	1101	a^5	0110	0001	1111
$(a+1)^6$	1000	a^6	1100	1111	1000
$(a+1)^7$	0111	a^7	1011	1000	0100
$(a+1)^8$	1001	a^8	0101	0100	0010
$(a+1)^9$	0100	a^9	1010	0010	0001
$(a+1)^{10}$	1100	a^{10}	0111	0001	1111
$(a+1)^{11}$	1011	a^{11}	1110	1111	1000
$(a+1)^{12}$	0010	a^{12}	1111	1000	0100
$(a+1)^{13}$	0110	a^{13}	1101	0100	0010
$(a+1)^{14}$	1010	a^{14}	1001	0010	0001

Таким образом, строка матрицы M_r представляет собой остаток от деления полинома $(X+1)^{j/t-(s-1)p/t}$ на полином g(X), где j- значение степени эквивалентного элемента $(a+1)^j = (a+1)^i$, которое нацело делится на t; t- значение степени элемента поля $GF(2^m)$ над полиномом g(X), для которого h(X) является минимальным полиномом: a^s - начальное состояние РСЛОС ГТП; p, n- показатели полиномов соответственно y(X) и g(X).

Итак, аналитический расчет значений сигнатур для непримитивных полиномов РСЛОС АТР отличается только способом построения матрицы для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР. Поэтому вывод о том, что сигнатура конъюнкции с рангом r<m-w, где w- вес числа -k, равна нулю, выполняется и в данном случае.

2. Анализ порождающих полиномов РСЛОС ГТП и АТР кратной степени

Если degg(X)<degh(X)=m, то рассмотренный алгоритм построения матрицы M_k неприменим, поскольку построить поле $GF(2^m)$ над неприводимым полиномом g(X) можно только в случае, когда степень g(X) не меньше m.

В связи с этим при анализе полиномов g(X) со степенью, меньшей степени h(X), значения сигнатур будем рассматривать в обозначениях поля $GF(2^m)$ над полиномом h(X): если сигнатура в базисе элементов поля над полиномом g(X) равна нулю, она равна нулю и в базисе элементов поля над полиномом h(X). В этом случае нет необходимости в переходе от значений РСЛОС ГТП к значениям РСЛОС АТР, а, следовательно, и в построении матрицы M_k .

Утверждение 1. Пусть h(X)- примитивный полином, g(X)- неприводимый полином, degh(X)=m, degg(X)=n, причем m/n=z, z- натуральное число. Тогда вес w(-k) числа -k принимает максимальное значение, равное m-z при $k=(2^m-1)/(2^n-1) = 2^{(z-1)n}+2^{(z-2)n}+...+2^n+1;$ сигнатура конъюнкции с рангом r<z равна нулю; w(-k)

принимает минимальное значение, равное z при $k=-(2^m -1)/(2^n -1)$, сигнатура конъюнкции с рангом r<m-z равна нулю.

Доказательство. Поскольку n делит m нацело, поле $GF(2^n)$ является подполем $GF(2^m)$, поэтому корни полиномов h(X) и g(X) связаны между собой соотношением $b=a^k$.

Число w(-k) представляет собой вес числа -k, поэтому, чем меньше количество единиц в двоичном представлении k, тем w больше. Минимальное значение числа k равно при максимальном значении показателя полинома g(X). Максимальный показатель g(X) соответствует примитивному полиному и равен $(2^n - 1)$.

Прежде всего докажем, что

$k=(2^m -1)/(2^n -1) = 2^{(z-1)n} +2^{(z-2)n} +...+2^n +1$ (1) ,

при n>1 (случай при n=1 рассмотрим отдельно). В соответствии с методом математической индукции , вначале проверим выполнение этого равенства при z=2 (при z=1 равенство (1) очевидно): m=2n;

$(2^{2n} -1)/(2^n -1)=2^n +1$; $(2^{2n} -1)=(2^n -1)(2^n +1)=2^{2n} -1$, таким образом, равенство выполняется.

Предположим, что выражение (1) справедливо при z. Покажем, что оно выполняется при (z+1):

$(2^{(z+1)n} -1)/(2^n -1)=2^{zn} +2^{(z-1)n} +2^{(z-2)n} +...+2^n +1$,

или $(2^{(z+1)n} -1)/(2^n -1)=2^{zn} +(2^{zn} -1)/(2^n -1)$;

$2^{(z+1)n} -1=2^{zn} (2^n -1)+2^{zn} +1$; $2^{(z+1)n} -1=2^{(z+1)n} -2^{zn} +2^{zn} -1=2^{(z+1)n} -1$.

Таким образом, число k в двоичном представлении при максимальном показателе g(X) $2^n -1$ содержит z единиц. Это количество единиц является минимальным. Поскольку показатель полинома вычисляется согласно выражению [6] : $e=(2^m -1)/НОД(2^m -1, k)$, то другие значения показателей g(X) получаются при делении $2^n -1$ на простые сомножители числа $2^n -1$. Поэтому, числа k, соответствующие этим показателям, равны числу $(2^m -1)/(2^n -1)$, умноженному на соответствующее простое число j. В результате такого умножения количество единиц в двоичном представлении числа k только увеличивается и равно zw(j), где w(j)- вес числа j в двоичном представлении.

Поскольку $(2^m -1)/(2^n -1)$ в двоичном представлении содержит минимальное количество единиц, то $-(2^m -1)/(2^n -1)$ содержит максимальное количество единиц. При этом w(-k) принимает минимальное значение.

Рассмотрим случай, когда n=1. При этом $k=(2^m -1)=0$, что соответствует полиному X+1. В этом случае w принимает два значения: если k считать равным $(2^m - 1)$, w(-k)=0, если k считать равным 0, w(-k)=m. Это соответствует особому поведению полинома X+1: сигнатура конъюнкций с рангом 0<r<m равна нулю.

Следующее утверждение для случая, когда разрядность РСЛОС АТР больше разрядности РСЛОС ГТП, приведем без доказательства.

Утверждение 2. Пусть h(X), g(X)- неприводимые полиномы, dtgh(X)=m, degg(X)=n, n/m=z, z- натуральное число, причем z>1, если h(X)- примитивный, z>0, если h(X)- непримитивный. При длине тестовой последовательности, равной показателю полинома g(X), сигнатура любой конъюнкции равна нулю, и , следовательно, все неисправности КС (за исключением неисправностей, преобразующих КС в последовательностную схему) являются необнаруживаемыми.

Заключение

На основании приведенных утверждений можно выполнить простую сравнительную оценку различных сочетаний порождающих полиномов РСЛОС ГТП и АТР. Например, для $h(X)=X^{10} + X^3 +1$:

1) при $g(X)=X^{10} +X^3 +1$ z=1, сигнатура конъюнкции с рангом r<1 равна нулю;

2) при $g(X)=X^5+X^4+X^3+X^2+1$ $z=2$, $k=(2^{10}-1)/(2^5-1)=33$, поэтому w принимает максимальное значение для degg(X)=5 и degh(X)=10, равное 10-2=8, сигнатура конъюнкции с рангом r<2 равна нулю;

3) при $g(X)=X^5+X^4+X^2+X+1$ $z=2$, $k=33*3=99$, поэтому w принимает меньшее значение для degg(X)=5 и degh(X)=10, равное 10-4=6, сигнатура конъюнкции с рангом r<4 равна нулю;

4) при $g(X)=X^5+X^2+1$ $z=2$, $k=1023-165=858$, поэтому w принимает еще меньшее значение для degg(X)=5 и degh(X)=10, равное 10-6=4, сигнатура конъюнкции с рангом r<6 равна нулю;

5) при $g(X)=X^5+X^3+X^2+X+1$ $z=2$, $k=-(2^{10}-1)/(2^5-1)=-33$, поэтому w принимает минимальное значение для degg(X)=5 и degh(X)=10, равное 2, сигнатура конъюнкции с рангом r<10-2=8 равна нулю;

6) при $g(X)=X^2+X+1$ $z=5$, $k=(2^{10}-1)/(2^2-1)=341$, поэтому w принимает максимальное значение для degg(X)=2 и degh(X)=10, равное 10-5=5, сигнатура конъюнкции с рангом r<5 равна нулю.

Из приведенных вариантов сочетаний порождающих полиномов наилучшим с точки зрения обеспечения сигнатурной тестируемости является первый, при этом разрядность РСЛОС АТР равна 10. При разрядности РСЛОС АТР равной 5 из рассмотренных четырех вариантов примитивных полиномов наилучшим является второй, причем четвертый и пятый варианты являются хуже шестого, для которого разрядность РСЛОС АТР равна 2. Кроме того, следует отметить, что, как правило, для минимальной аппаратной реализации порождающие полиномы для РСЛОС ГТП и АТР выбирают с минимальным количеством ненулевых коэффициентов. Такие полиномы, в частности, в таблице неприводимых полиномов [6] расположены на первом месте. Рассмотренный пример показывает, что для разрядности РСЛОС ГТП и АТР соответственно 10 и 5, выбор первых полиномов для (псевдо-исчерпывающего тестирования КС (четвертый вариант сочетаний полиномов) является менее эффективным по сравнению с разрядностью РСЛОС ГТП и АТР соответственно 10 и 2.

Полученные результаты могут найти применение при реализации самотестирования цифровых схем, проектировании схем встроенного контроля и диагностирования, при компактном тестировании КС.

Литература

1. Ярмолик В.Н. Аналитический метод вычисления сигнатур для сетевых дискретных структур// АВТ.- 1987.-N5.-С.77-81.
2. Ярмолик В.Н., Калоша Е.П. Метод аналитического расчета сигнатур 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. Дяченко О.Н. Метод аналитического вычисления сигнатур// Сборник трудов факультета вычислительной техники и информатики. Выпуск 1..- Донецк: ДонГТУ, 1996.-С.97-102.
5. Дяченко О.Н. Сравнительная оценка эффективности методов компактного тестирования комбинационных схем// Сборник трудов факультета вычислительной техники и информатики. Выпуск 1..- Донецк: ДонГТУ, 1996.-С.103-110.
6. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ.-М.: Мир.-1976.- 595с.