КОМПАКТНОЕ ТЕСТИРОВАНИЕ НА ОСНОВЕ ЧЕТЫРЕХЗНАЧНОЙ ЛОГИКИ

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

Abstract

Dyachenko O.N., Gerasimov A.N. Compact testing on the basis four-valued logic. *Problems on the using of linear shift feedback registers (LSFR) based on four-valued logic for compact testing digital circuits are considered. The algorithm for determination of primitive polynomials on GF(4) is suggested. A table of some primitive polynomials on GF(4) is presented. The advantages of LSFR GF(4) as compared with LSFR GF(2) is described The obtained results may be of use to self-testig circuit design, compact testing built-in testing of digital circuits on the basis two-valued as well as four-valued logic.*

Увеличение сложности и функциональной насыщенности цифровых устройств средств вычислительной техники приводит к значительным трудностям при решении задач их контроля и диагностирования. В связи с этим в области технической диагностики появилось и в последние годы интенсивно развивается такое направление научных исследований как контролепригодное проектирование цифровых устройств. В настоящее время в арсенале контролепригодного проектирования насчитывается целый ряд подходов и методов решения задач синтеза легко тестируемых схем. Одним из таких подходов является введение в схемы встроенных средств тестирования.

Для обеспечения минимальной аппаратной избыточности встроенные средства тестирования, как правило, предполагают компактную генерацию тестовых воздействий и компактный анализ тестовых реакций. Применение методов компактного тестирования (КТ) ставит задачу определения достоверности результатов тестового эксперимента. Это обстоятельство предопределило существование целого ряда различных способов аппаратной реализации компактного тестирования. Использование линейных переключательных схем для целей КТ является наиболее совместимым с методом сквозного сдвигового регистра (LSSD - Level Sensitive Scan Design)[1]. Метод LSSD - предполагает декомпозицию схемы в режиме тестирования на несколько сдвиговых регистров и комбинационные схемы благодаря применению специальных элементов памяти. При этом задача тестирования цифрового устройства сводится в основном к проверке комбинационной части.

С помощью незначительных схемных изменений сдвиговые регистры преобразуются в регистры сдвига с линейными обратными связями (РСЛОС), которые могут выполнять функции генераторов псевдослучайной тестовой последовательности (ГПТП) и анализаторов тестовых реакций (АТР).

В работах [2,3,4] выполнен подробный анализ эффективности и особенностей применения РСЛОС в качестве ГПТП и АТР, построенных на основе двузначной логики. Вместе с тем подобные структуры могут быть разработаны на основе k-значной логики. Для простых чисел k такие структуры рассмотрены в работах, посвященных КТ, в частности, в [5]. Такое ограничение, вероятно, связано с определением поля Галуа, приведенным в [6]. Вместе с тем, поля Галуа существуют и для кратных k [7]. В данной работе предлагается использование для целей КТ линейных переключательных схем , построенных на основе четырехзначной логики.

Как и в случае двузначной, устройства КТ k - значной логики представляют собой линейные переключательные схемы для деления полиномов. Обратные связи выбираются в соответствии с ненулевыми коэффициентами образующего полинома (полинома - делителя). Один из важных вопросов аппаратной реализации устройства компактного тестирования - выбор образующего полинома. Как правило в качестве образующего полинома принимают неприводимый примитивный полином. Достоинства примитивного полинома: во первых для ГПТП такой полином обеспечивает генерацию псевдослучайной последовательности максимальной длины k^r - 1, где k - значность логики, r - степень полинома; для АТР - обнаружение всех одиночных ошибок независимо от длины анализируемой последовательности, обнаружение всех двукратных, если длина анализируемой последовательности не более $(k^r - 1)/(k - 1)$.

Примитивные полиномы двузначной логики определяют с помощью таблиц неприводимых полиномов. В [6,7] приведены неприводимые полиномы степени, не превосходящей 34, над полем GF(2), в [6] - неприводимые полиномы над полем GF(3), GF(5), GF(7) степени, не превосходящей соответственно 7,5,4.

Для определения примитивного полинома над полем GF(4) можно использовать алгоритм, который рассмотрим на примере.

Поле GF(4) содержит четыре элемента {0,1,2,3}. Операции сложения и умножения элементов поля GF(4) представлены в таблицах 1 и 2.

Таблица 1.

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Таблица 2.

*****	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Следует отметить что в отличие, от случаев когда k - простое число, операции сложения и умножения элементов поля GF(4) не являются сложением и умножением по модулю 4. Операция сложения может быть представлена как поразрядная сумма по модулю два при обозначении каждого элемента поля GF(4) двумя символами двузначной логики. Например $2 + 3 = 10 + 11 = 01 = 1$. Поэтому, как и в случае поля GF(2), операция вычитания в поле GF(4) эквивалентна операции сложения [7].

Предположим, требуется определить примитивный полином над полем GF(4) степени 2. Для построения такого полинома используем поле GF(16), которое является расширением поля GF(2) над примитивным полиномом четвертой степени, например $S(X) = X^4 + X + 1$. В поле GF(16) поле GF(4) можно представить в виде: $GF(4) = \{0, 1, 2, 3\} = \{0, 1, a^5, a^{10}\}$, где a - примитивный элемент поля GF(16). Множество сопряженных элементов, содержащих a, относительно GF(2) имеет вид $\{a, a^2, a^4, a^8\}$; относительно GF(4) - $\{a, a^4\}$. Поэтому искомый примитивный полином: $f_1(X)=(X-a)(X-a^4)=X^2-aX-aX^4-a^5=X^2+(a+a^4)X+a^5$.

Поскольку $S(X) = X^4 + X + 1$, и a - примитивный элемент поля GF(16), построенного над этим полиномом, выполняется равенство $a^4=a+1$. Следовательно, $f_1(X)=X^2+(a+a+1)X+a^5=X^2+X+a^5=X^2+X+2$.

Если поле GF(16) рассматривать как расширение поля GF(2) над другим примитивным полиномом, например $S'(X)= X^4 + X^3 + 1$, ($S'(X)$ - двойственный полином $S(X)$), получим $f_2(X)= X^2+(a+a^4)X+a^5.= X^2+(a+a^3+1)X+a^5=X^2+2X+2$. поскольку $a^3+a+1=a^5$ (остаток при делении полинома X^5 на полином $X^4 + X^3 + 1$ равен $X^3 + X + 1$.

Отметим, что $f_2(X)$ не является двойственным по отношению к $f_1(X)$: $f_1{}'(X)=X^{\deg f1(X)}*f_1(X)=X^2(X^{-2}+X^{-1}+2)=2X^2+X+1=X^2+3X+3$.

Аналогично получаем $f_2{}'(X)=X^2(X^{-2}+2X^{-1}+2)=2X^2+2X+1= X^2+X+3$.

Таким образом, получили четыре примитивных полинома над полем GF(4), поскольку двойственный полином по отношению к примитивному полиному также является примитивным: X^2+X+2, X^2+2X+2, X^2+3X+3, X^2+X+3.

Число $M(k,r)$ примитивных полиномов r-й степени над полем GF(k) можно определить согласно следующему выражению [6]: $M(k,r)=[L(k^r-1)]/r$, где $L(k^r-1)$ - число различных взаимно простых k^r-1 положительных чисел, меньших k^r-1, включая 1. В случае $k = 4$ и $r = 2$ получаем $M(4,2) = [L(4^2-1)]/2=8/2=4$. Таким образом выше приведены все примитивные полиномы второй степени над полем GF(4).

Аналогичным образом можно получить примитивные полиномы над GF(4) - произвольной степени r, используя примитивные над GF(2) степени $2r$. Например для $r = 8$ и примитивного полинома над GF(2) $X^{16}+X^{12}+X^3+X+1$ получаем примитивный полином над GF(4): $X^8+X^6+X^4+X^3+X^2+X+2$ и двойственный к нему $X^8+3X^7+3X^6+3X^5+3X^4+3X^2+3$. При этом $M(4,r) = 2M(2,2r)$, поскольку $L(4^r- 1) = L(2^{2r}- 1)$. Таким образом, в общем случае количество различных примитивных полиномов над GF(4) степени r вдвое больше различных примитивных полиномов над GF(2) степени 2r. Аналогично, M(8,r) = 3M(2,3r) и т.д.

В таблице 3 приведены некоторые примитивные полиномы над полем GF(2) степени 16 и соответствующие им примитивные полиномы над полем GF(4) степени 8, полученные с помощью программной реализации вышеизложенного алгоритма.

Таблица3.

Примитивный полином над полем GF(2)	*Примитивные полиномы над полем GF(4)*
$X^{16}+X^{15}+X^{14}+X^{11}+X^{10}+X^{5}+1$	$X^{8}+2X^{7}+X^{4}+2X^{2}+2$
$X^{16}+X^{15}+X^{10}+X^{8}+X^{6}+X^{5}+1$	$X^{8}+2X^{7}+3X^{6}+3X^{5}+2$
$X^{16}+X^{14}+X^{12}+X^{10}+X^{9}+X^{5}+1$	$X^{8}+3X^{6}+X^{5}+2X^{3}+2$
$X^{16}+X^{14}+X^{12}+X^{9}+X^{6}+X^{2}+1$	$X^{8}+X^{7}+X^{6}+2X+2$
$X^{16}+X^{14}+X^{10}+X^{7}+X^{4}+X^{2}+1$	$X^{8}+X^{7}+2X^{2}+2X+2$
$X^{16}+X^{12}+X^{11}+X^{6}+X^{5}+X^{3}+X^{2}+X+1$	$X^{8}+3X^{4}+3X^{3}+X+2$
$X^{16}+X^{11}+X^{10}+X^{8}+X^{6}+X+1$	$X^{8}+3X^{3}+3X^{2}+X+2$
$X^{16}+X^{11}+X^{7}+X^{6}+X^{4}+X^{2}+1$	$X^{8}+X^{5}+2X^{3}+3X^{2}+2$
$X^{16}+X^{10}+X^{9}+X^{8}+X^{6}+X^{5}+X^{3}+X^{2}+1$	$X^{8}+X^{3}+2X^{2}+2X+2$
$X^{16}+X^{10}+X^{6}+X^{5}+X^{2}+X+1$	$X^{8}+X^{6}+2X^{4}+X+2$

Следует отметить, что для каждого из приведенных полиномов над полем GF(4) можно определить еще три полинома над полем GF(4) . Например, полиному $X^8+X^7+X^6+2X+2$ соответствует двойственный ему полином $X^8+X^7+3X^2+3X+3$; подстановкой вместо коэффициентов 3 коэффициентов 2 получаем полином $X^8+X^7+2X^2+2X+2$, который соответствует двойственному полиному над GF(2): и наконец, последнему полиному соответствует двойственный ему полином $X^8+X^7+X^6+3X+3$.

Аппаратная реализация ГПТП и АТР четырехзначной логики основана на применении РСЛОС, выполняющих операцию деления на образующий полином . РСЛОС GF(4) в отличие от РСЛОС GF(2) в качестве элементов задержки использует два элемента памяти двоичной логики. Кроме того (при соответствии элементов GF(4) элементам GF(2) : 0 - 00 , 1 - 01 , 2 - 10 , 3 - 11) , элементы умножения и сложения GF(4) в двоичной логике реализуются следующим образом: (*1) - $y_1=x_1$; $y_2=x_2$; (*2) - $y_1=x_1+x_2$; $y_2=x_1$; (*3) - $y_1=x_2$; $y_2=x_1+x_2$; (+) - $y_1=x_1+x_3$; $y_2=x_2+x_4$; где в скобках обозначены операции, x_1, x_2, x_3, x_4 - разряды входных переменных, y_1, y_2 - разряды результата.

На рис 1.а, б приведены РСЛОС GF(4) для АТР и ГПТП соответственно, образующий полином X^2+X+2. Обратные связи выбираются в соответствии с ненулевыми коэффициентами полинома. На рис.1.в приведена схема ГПТП поля GF(4) на элементах двоичной логики, на рис.1.г - та же схема в виде одного регистра с обратными связями. При начальном ненулевом состоянии ГПТП генерирует псевдослучайную последовательность, период которой равен $4^2 - 1 = 15$. Если начальное состояние ГПТП соответствует элементу поля a^0, т.е. 1, то генерируемая последовательность имеет вид a^0 , a^1, ..., a^{14} .

В таблице 4 представлено поле GF(16) как расширение поля GF(4) над полиномом $X^2 + X + 2$ и как расширение поля GF(2) над полиномом $X^4 + X + 1$.

Обозначим элементы поля a^0, a^1, ..., a^{14} в двоичном виде для расширения поля GF(4)

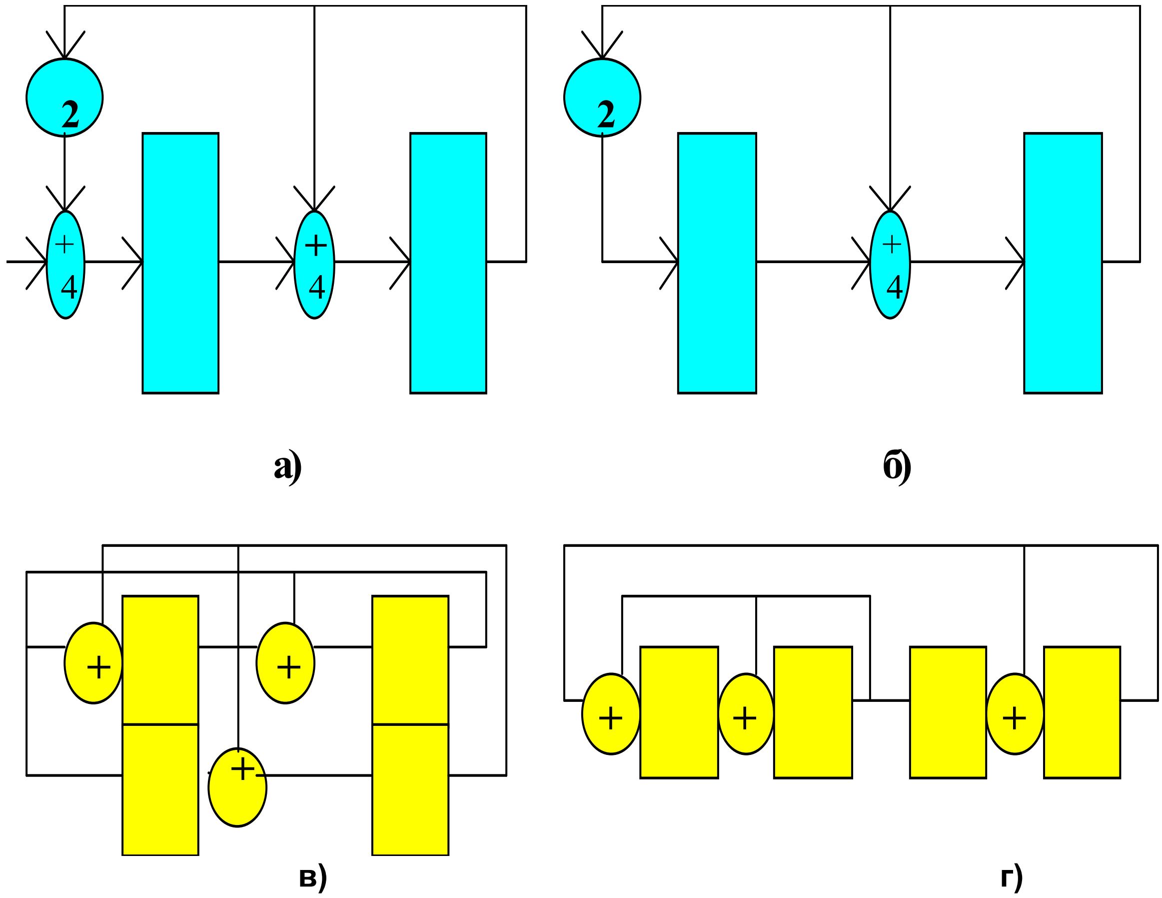

Рис. 1 . РСЛОС GF(4) и GF(2) для АТР и ГПТП

$Z=z_3z_2z_1z_0$; для расширения поля GF(2) - $X=x_3x_2x_1x_0$. Анализ таблицы показывает, что $z_3=x_3$, $z_2=x_2+x_1$, $z_1=x_3+x_2$, $z_0=x_0$, или $Z=M*X$, где M- матрица, строки которой представляют собой двоичное представление элементов a^0, a^1, a^2, a^3 расширения поля GF(4) над полиномом $X^2 + X + 2$. Таким образом, для определения зависимости Z от X достаточно построить матрицу из элементов a^0, ... , a^{2r-1} , где r - степень полинома над полем GF(4). Поскольку Z и X - состояния РСЛОС GF(4) и GF(2) при генерации псевдослучайной последовательности или сжатии тестовой реакции, из полученной зависимости следует, что обнаруживающие способности АТР в виде РСЛОС GF(2) с образующим полиномом степени 2r равны обнаруживающим способностям АТР в виде РСЛОС GF(4) с образующим полиномом степени r, который получен на основе сравниваемого полинома над полем GF(2).

В заключение можно сделать следующие выводы:

- РСЛОС, построенные на основе четырехзначной логики, как и РСЛОС двузначной логики, хорошо сочетаются с методом сквозного сдвигового регистра;
- аппаратная реализация в двоичной логике РСЛОС над полем GF(4) сравнима по затратам с РСЛОС над полем GF(2);
- количество примитивных полиномов степени r над полем GF(4) в два раза больше количества примитивных полиномов степени 2r над полем GF(2), что позволяет реализовать в два раза больше различных ГПТП максимального периода;
- обнаруживающие способности АТР на основе РСЛОС четырехзначной логики для ошибок разной кратности равны обнаруживающим способностям АТР на основе РСЛОС двоичной логики;
- РСЛОС, построенные на основе многозначной логики могут найти применение для компактного тестирования цифровых устройств как двоичной, так и многозначной логики.

Таблица 4.

Расширение поля GF(4)			*Расширение поля GF(2)*
В виде степени	В 4-м виде	В 2-м виде	В 2-м виде
0	00	0000	0000
a^0	01	0001	0001
a^1	10	0100	0010
a^2	12	0110	0100
a^3	32	1110	1000
a^4	11	0101	0011
a^5	02	0010	0110
a^6	20	1000	1100
a^7	23	1011	1011
a^8	13	0111	0101
a^9	22	1010	1010
a^{10}	03	0011	0111
a^{11}	30	1100	1110
a^{12}	31	1101	1111
a^{13}	21	1001	1101
a^{14}	33	1111	1001

Таким образом, главным преимуществом РСЛОС, построенных на основе примитивных полиномов над полем GF(4), является возможность реализации большего количества различных ГПТП максимального периода. Результаты моделирования РСЛОС GF(4) на элементах двоичной логики с порождающими полиномами из таблицы 3 с помощью САПР OrCAD подтверждают примитивность этих полиномов: ГПТП в виде РСЛОС GF(4) генерируют 4^8-1 различных наборов при начальном ненулевом состоянии РСЛОС.

ЛИТЕРАТУРА

1. Беннетс Р.ДЖ. Проектирование тестопригодных логических схем: Пер. с англ. - М.: Радио и связь, 1990. - 176 с.
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. Сравнительная оценка эффективности методов компактного тестирования комбинационных схем. Сборник трудов факультета вычислительной техники и информатики. Выпуск 1. Донецкий государственный технический университет. - Донецк: ДонГТУ, 1996. - 215с.
5. Литиков И.П. Кольцевое тестирование цифровых устройств.- М.: Энергоатомиздат, 1990.- 160с.
6. Линейные последовательностные машины. Гилл А., пер. с англ. Издательство "Наука" Главная редакция физико-математической литературы, М., 1974, 288 с.
7. Питерсон У. Уэлдон Э. Коды исправляющие ошибки. - М.: Мир, 1976. - 600с.