

КОМПАКТНЫЙ АНАЛИЗ НАД ПОЛЕМ GF(3)

Дяченко О.Н.

Кафедра ЭВМ ДонНТУ
don@cs.dgtu.donetsk.ua

Abstract

Dyachenko O.N. Compact analysis over field GF(3). The features signature analysis is discussed for the case of using characteristic polynomials over GF(3) for linear feedback shift registers. One of the approaches of the compact analysis - signature-syndromic testing grounded on operations of division by polynomials over a field GF(2) - is spread in area of polynomials over a field GF(3).

Введение

Методам компактного тестирования принадлежит значительная роль при решении задач снижения трудоёмкости контроля и диагностики сложных цифровых устройств. Среди широкого спектра различных способов компактного тестирования сигнатурный анализ обладает рядом преимуществ: простая аппаратная реализация, высокое быстродействие сигнатурных анализаторов, простая аппаратная реализация многоканальных анализаторов тестовых реакций, высокие обнаруживающие способности. Традиционный сигнатурный анализ основан на операции деления полиномов над полем GF(2), причём в качестве делимого выступает анализируемая последовательность, представленная в виде полинома над полем GF(2), в качестве делителя - порождающий полином над полем GF(2), в соответствии с ненулевыми коэффициентами которого выбираются обратные связи регистра сдвига с линейными обратными связями. Таким образом, анализируемая тестовая реакция представляется последовательностью логических нулей и единиц. Вместе с тем логические анализаторы, как правило, позволяют определять в контрольных точках не только уровни логического нуля или логической единицы, но также неопределённое состояние, которому может соответствовать либо уровень напряжения, меньший уровня логической единицы и больший уровня логического нуля, либо высокоимпедансное состояние логического элемента с тристабильными выходами, либо отсутствие контакта щупа с контрольной точкой. В этом случае анализируемую тестовую реакцию можно представить в виде последовательности трёхзначных символов, например, 0 - логический ноль, 1 - логическая единица, 2 - неопределённое состояние.

В [1] рассмотрены вопросы аппаратной реализации РСЛОС с порождающими полиномами над полем GF(3) на элементах двоичной логики. В данной работе предлагается один из подходов компактного анализа - сигнатурно-синдромное тестирование, основанное на операции деления полиномов над полем GF(3).

1. Особенности сигнатурного анализа над полем GF(3)

РСЛОС с порождающим полиномом над полем GF(3) (РСЛОС GF(3)) имеет более сложную аппаратную реализацию по сравнению с РСЛОС GF(2). Однако сигнатурный анализ на основе РСЛОС GF(3) обладает повышенными контролирующими способностями, поскольку наряду с возможными логическими нулями и единицами учитывает возможные ситуации неопределённого состояния.

Как и в случае GF(2), для РСЛОС GF(3) обратные связи целесообразно выбирать в соответствии с ненулевыми коэффициентами неприводимого примитивного порождающего полинома над полем GF(3). Полином выбирается примитивным, поскольку в этом случае можно получить максимальное количество всевозможных остатков от деления на такой полином, равное 3^n , а следовательно, максимально возможное количество различных сигнатур.

Рассмотрим особенности сигнатурного анализа над полем GF(3). Аналогично полю GF(2) анализируемую тестовую реакцию троичных символов можно представить в виде полинома над полем GF(3):

$$f(X) = f_n X^n + f_{n-1} X^{n-1} + \dots + f_1 X + f_0,$$

где X - неопределённая (фиктивная) переменная, коэффициенты f_i принадлежат полю GF(3) (т.е. могут принимать значения 0, 1, 2), знак "+" обозначает операцию по модулю 3. Например, троичную последовательность 12020102 можно представить в виде полинома $X^7 + 2X^6 + 2X^4 + X^2 + 2$.

Как и в случае GF(2), в поле GF(3) выполняется принцип суперпозиции:

$$S[A(X) + B(X)] = S[A(X)] + S[B(X)],$$

т.е. сигнатура суммы по модулю 3 двух полиномов над полем GF(3) (X) и B(X) равна посимвольной сумме по модулю три сигнатур A(X) и B(X). Сигнатуры представляют собой остаток от деления соответствующего полинома на порождающий полином РСЛОС сигнатурного анализатора.

Обозначим: A(X) - эталонная тестовая реакция, B(X) - реальная тестовая реакция, т.е. тестовая реакция с ошибками, E(X) - полином ошибки. Тогда

$$A(X) - B(X) = E(X).$$

Следует отметить, что в отличие GF(2), в поле GF(3) операция вычитания не эквивалентна операции сложения.

Например, предположим, что эталонная тестовая реакция имеет вид 120120120, а реальная - 201012120, тогда вектор ошибки будет иметь вид 222111000, при этом символы 2 и 1 означают отличие, символ 0 - совпадение эталонной и реальной тестовых реакций. Посимвольная сумма по модулю три вектора ошибки и реальной тестовой реакции равна эталонной тестовой реакции:

$$201012120 + 222111000 = 120120120,$$

или в полиномиальной форме представления:

$$A(X) = B(X) + E(X).$$

Согласно принципу суперпозиции

$$S[A(X) - B(X)] = S[E(X)] = S[A(X)] - S[B(X)],$$

$$S[A(X)] = S[B(X)] + S[E(X)].$$

Итак, для сигнатурного анализа над полем GF(3) в отличие от поля GF(2) существует два типа ошибок: 1 - появление вместо 1 - 0, вместо 2 - 1, вместо 0 - 2; 2 - появление вместо 1 - 2, вместо 2 - 0, вместо 0 - 1.

Рассмотрим структуру поля $GF(3^n)$ на примере расширения поля $GF(3)$ по примитивному полиному над полем $GF(3)$ X^2+X+2 (см.табл.1). Следует отметить, что все ненулевые элементы можно разделить на два подмножества: a^0, a^1, a^2, a^3 и a^4, a^5, a^6, a^7 , где a –примитивный элемент поля. Элементы этих подмножеств являются линейно зависимыми. Во-первых, второе подмножество можно получить из первого заменой символов 1(2) на 2(1); во-вторых, посимвольная сумма по модулю три i -х элементов подмножеств равна 0. Аналогичную структуру имеет любое поле $GF(3^n)$, полученное как расширение $GF(3)$ по примитивному полиному над полем $GF(3)$.

Таблица 1 - Поле $GF(3^2)$.

| Элементы поля $GF(9)$ | |
|-----------------------|--------------------------|
| в виде степени | в виде троичных символов |
| 0 | 00 |
| a^0 | 01 |
| a^1 | 10 |
| a^2 | 21 |
| a^3 | 22 |
| a^4 | 02 |
| a^5 | 20 |
| a^6 | 12 |
| a^7 | 11 |

2. Компактный анализ над полем $GF(3)$ в виде сигнатурно-синдромного тестирования

Рассмотрим особенности сигнатурно-синдромного тестирования над полем $GF(3)$ - частного случая сигнатурного анализа комбинационных схем (КС). Сигнатурно-синдромное тестирование над полем $GF(2)$ [2,3] предполагает исчерпывающее тестирование КС, применение в качестве генератора тестовых воздействий - двоичного счётчика и сигнатурно-синдромного анализатора тестовых реакций.

Достоинства сигнатурно-синдромного тестирования (ССТ) КС следующие. Во-первых, ССТ позволяет выполнять аналитический расчёт значений сигнатурных синдромов и, в частности, по известным значениям сигнатурных синдромов на независимых входах логического элемента определять значение сигнатурного синдрома на его выходе. На основе аналитического расчёта значений сигнатурных синдромов возможна комплексная оценка достоверности результатов тестового эксперимента, которая учитывает не только обнаруживающие способности анализатора тестовых реакций, но также характер тестовых воздействий и тестовых реакций в зависимости от конкретных неисправностей объекта диагностики. Например, в [4] на основе свойств сигнатурного синдрома доказано обнаружение всех неисправностей определённого класса неисправностей [4] в программируемых логических матрицах при применении анализатора в виде РСЛЮС с примитивным порождающим полиномом минимальной степени X^2+X+1 .

Во-вторых, при задании начального состояния РСЛОС сигнатурно-синдромного анализатора, равного эталонной сигнатуре, появляется возможность локализовать одиночную ошибку в анализируемой тестовой последовательности, т.е. указать порядковый номер искажённого символа.

Основой сигнатурно-синдромного анализатора [3,5] над полем GF(2) (ССА GF(2)) является РСЛОС с порождающим примитивным полиномом над полем GF(2) и двоичный счётчик. Принцип работы ССА GF(2) заключается в следующем. В РСЛОС производится сжатие тестовой реакции, по окончании которого РСЛОС продолжает свою работу до появления во всех его разрядах, кроме первого, нулей, т.е. до состояния РСЛОС, равного "100...0". Двоичный счётчик подсчитывает количество тактов с момента окончания сжатия тестовой реакции, и его показания определяют значение сигнатурного синдрома, если начальное состояние РСЛОС равно нулю, или номер одиночного искажённого символа, если начальное состояние РСЛОС равно эталонной сигнатуре.

2.1 Локализация одиночного ошибочного троичного символа

Вначале рассмотрим сигнатурно-синдромный анализатор над полем GF(3) (ССА GF(3)) с возможностью локализации одиночного ошибочного троичного символа при ССТ над полем GF(3) КС двоичной логики. Отличительная особенность ССА GF(3) - применение РСЛОС GF(3) вместо РСЛОС GF(2). Кроме того, учитывая, что возможны два состояния РСЛОС GF(3), при которых все его разряды, кроме первого, равны нулю: "100...0" и "200...0" (см. табл. 1), если длина анализируемой последовательности равна 3^n-1 , следует её ограничить до значения $(3^n-1)/2$. И, наконец, последняя отличительная особенность - начальное состояние РСЛОС GF(3). Оно должно быть таким, чтобы по окончании сжатия тестовой реакции без ошибок состояние РСЛОС приняло нулевое значение. Тогда при сжатии тестовой реакции с ошибкой, согласно принципу суперпозиции, РСЛОС примет состояние, равное сигнатуре вектора ошибки.

В РСЛОС GF(2) с начальным состоянием, равным эталонной сигнатуре $S[A(X)]$, определённой для длины тестовой реакции 2^n-1 , через 2^n-1 тактов его состояние вновь станет равным $S[A(X)]$, если на информационном входе РСЛОС GF(2) - константа ноль. Тогда при сжатии тестовой реакции без ошибок согласно принципу суперпозиции состояние РСЛОС GF(2) станет равным нулю: $S[A(X)]+S[A(X)]=0$, где знак '+' означает посимвольную сумму по модулю 2.

В РСЛОС GF(3) с начальным состоянием, равным эталонной сигнатуре $S[A(X)]$, определённой для длины тестовой реакции $(3^n-1)/2$, через $(3^n-1)/2$ тактов для константы ноль на информационном входе РСЛОС GF(3) станет равным $S'[A(X)]$, где знак ' (штрих) означает замену в $S[A(X)]$ символов 1(2) на 2(1) (см. табл. 1). Например, если эталонная сигнатура $S[A(X)]$ равна 120, то $S'[A(X)]=210$. Тогда при сжатии тестовой реакции без ошибок, длина которой равна $(3^n-1)/2$, состояние РСЛОС GF(3) также станет равным нулю: $S[A(X)]+S'[A(X)]=0$, где знак '+' означает посимвольную сумму по модулю три.

Таким образом, независимо от различия операций в РСЛОС GF(2) и РСЛОС GF(3), в обоих случаях их начальное состояние следует задавать равным эталонной сигнатуре. Тогда после окончания сжатия тестовой реакции с ошибкой содержимым РСЛОС будет $S[E(X)]$. ССА GF(3) продолжает свою работу до тех пор, пока в РСЛОС появится комбинация "100...0" или "200...0". Если ошибка одиночная, тогда показания счётчика - её порядковый номер.

Необходимо отметить, что ССА GF(3) можно применять для локализации одиночных ошибок в тестовой реакции для любого цифрового объекта диагностики и любого генератора тестовых воздействий.

2.2 Сигнатурно-синдромный анализатор над полем GF(3) с начальным нулевым состоянием

Рассмотрим ССА GF(3) с начальным нулевым состоянием РСЛОС. При тестировании КС двоичной логики и генераторе тестовых воздействий в виде двоичного счётчика ССА GF(3) не сохраняет свойства сигнатурного синдрома над полем GF(2). Эти свойства основаны на следующем равенстве в поле GF(2): $(X^i+1)^2=X^{2i}+1$, где знак "+" означает сложение по модулю два. В поле GF(3) это равенство не выполняется, однако справедливо следующее равенство $(X^i+1)^3=X^{3i}+1$, где знак "+" означает сложение по модулю три. Действительно, $(X^i+1)^3 = (X^i+1)(X^i+1)(X^i+1) = (X^{2i}+2X^i+1)(X^i+1) = X^{3i}+2X^{2i}+X^i+X^{2i}+2X^i+1 = X^{3i}+1$. Поэтому свойства сигнатурного синдрома будут выполняться для генератора тестовых воздействий в виде троичного счётчика, КС трёхзначной логики и ССА GF(3).

Аналитический расчёт значений сигнатурного синдрома над полем GF(3) (SS3) рассмотрим на примере. Предположим, что функция трёхзначной логики задана таблицей 2.

Запишем функцию в сигма-пи нормальной форме и минимизируем её (знак "*" означает умножение по модулю три, знак "+" означает сложение по модулю три) [6]:

$$f(V1, V2) = \Phi_0(V1) * \Phi_0(V2) + \Phi_1(V1) * \Phi_0(V2) * 2 + \Phi_1(V1) * \Phi_1(V2) + \Phi_2(V1) * \Phi_0(V2) * 2 + \Phi_2(V1) * \Phi_1(V2) * 2 + \Phi_2(V1) * \Phi_2(V2) * 2 = \Phi_0(V1) * \Phi_0(V2) + \Phi_1(V1) * \Phi_0(V2) * 2 + \Phi_1(V1) * \Phi_1(V2) + \Phi_2(V2) * 2.$$

Предположим, что ГТП реализуется на основе n-разрядного вычитающего троичного счётчика с начальным состоянием "22...2", длина тестовых воздействий равна 3^n , АТР - в виде ССА GF(3), РСЛОС которого прекращает работу при появлении состояния "100...0" или "000...0". Показания счётчика определяют значение сигнатурного синдрома над полем GF(3).

Таблица 2 - Функция трёхзначной логики.

| V1 V2 | f(V1, V2) | V1 V2 | f(V1, V2) |
|-------|-----------|-------|-----------|
| 0 0 | 1 | 1 2 | 0 |
| 0 1 | 0 | 2 0 | 2 |
| 0 2 | 0 | 2 1 | 2 |
| 1 0 | 2 | 2 2 | 2 |
| 1 1 | 1 | | |

Приведём без доказательства некоторые свойства SS3.

1. Сигнатурный синдром конъюнкции $\Phi_i(V_j)$ равен X^Y , где $Y = i * 3^{(n-j)} + a(3^{k_1-1} + 3^{k_2-1} + 3^{k_3-1} + \dots + 3^{k_i-1})$, причём k_1, k_2, \dots, k_i - индексы отсутствующих аргументов V_i ; a - характеристическое число порождающего полинома РСЛОС:

$SS3(X^2+X+1)=X^a$; знак "*" и "+" в выражении для Y означает арифметическое умножение и сложение.

2. Сигнатурный синдром конъюнкции $\Phi_{i1}(V1)*\Phi_{i2}(V2)*\dots*\Phi_{in}(Vn)$ равен X^Y , где $Y=i_1*3^{(n-1)}+i_2*3^{(n-2)}+\dots+i_n$.

3. Умножение на константу 2 соответствует умножению на X^Y , где $Y=(3^n-1)/2$.

4. $SS3(X^Y+1)=0$, где $Y=(3^n-1)/2$.

5. Если $SS3(X^Z+1)=X^t$, то $SS3(X^{3Z}+1)=X^{3t}$.

Для рассматриваемого примера предположим, что порождающий полином РСЛОС GF(3) равен X^2+X+2 . Определим соответствующие ему табличные значения логарифмов, аналогичные логарифмам Зеча в поле GF(2) ($SS3(X^Z+1)=X^t$):

$Z=1, t=7; Z=2, t=3; Z=3, t=1*3=3; Z=5, t=2; Z=6, t=3*3 \bmod 8=1; Z=7, t=6$.

Характеристическое число a полинома X^2+X+2 равно 4, поскольку $SS3(X^2+X+1)=X^4$.

Первый вариант аналитического расчёта $SS3[f(V1,V2)]$. Определим значения $\Phi_i(Vi)$ согласно первому свойству SS3:

$\Phi_0(V2) = X^4: y = (00)_3 + 4*(10)_3 = 4*3 = 12-8 = 4;$

$\Phi_1(V2) = X^5: y = (01)_3 + 4*(10)_3 = 1+12 = 13-8 = 5;$

$\Phi_2(V2) = X^6: y = (02)_3 + 4*(10)_3 = 2+12 = 14-8 = 6;$

$\Phi_0(V1) = X^4: y = (00)_3 + 4*(01)_3 = 4;$

$\Phi_1(V2) = X^7: y = (10)_3 + 4*(01)_3 = 3+4=7;$

$\Phi_2(V2) = X^2: y = (20)_3 + 4*(01)_3 = 6+4 = 10-8 = 2;$

$SS3[f(V1,V2)] = X^4X^4+X^7X^4X^4+X^5X^7+X^2X^4 = X^0+X^7+X^{12}+X^{-2} =$
 $= X^7+X^6+X^4+1 = X^7+X^6 = X^6(X+1) = X^7X^6 = X^{13-8} = X^5.$

Второй вариант аналитического расчёта $SS3[f(V1,V2)]$ основан на применении второго свойства SS3:

$SS3[f(V1,V2)] = X^{(00)} + X^{(10)}*X^{-4}+X^{(11)}+X^2X^{-4} = X^0+X^{3-4}+X^4+X^{-2} =$
 $= 1+X^{-1+8}+X^4+X^6 = X^7+X^6+X^4+1 = X^7+X^6 = X^7X^6 = X^{13-8} = X^5,$

(в данном случае скобки в степени означают троичную систему счисления).

В таблице 3 представлена проверка полученного результата: рассчитанный аналитически и табличный сигнатурные синдромы равны $SS3[f(V1,V2)] = X^5$.

Таблица 3 - Определение сигнатурного синдрома $SS3[f(V1,V2)]$

| ГТП V1 V2 | f(V1,V2) | РСЛОС CCA GF(3) | СТ CCA GF(3) |
|--------------|----------|--------------------|-----------------|
| 2 2 | 2 | 2 0 | |
| 2 1 | 2 | 2 2 | |
| 2 0 | 2 | 1 0 | |
| 1 2 | 0 | 0 1 | |
| 1 1 | 1 | 2 2 | |
| 1 0 | 2 | 1 0 | |
| 0 2 | 0 | 0 1 | |
| 0 1 | 0 | 1 2 | |
| 0 0 | 1 | 0 2 | |
| | | 2 0 | 1 |
| | | 2 2 | 2 |
| | | 1 2 | 3 |
| | | 0 1 | 4 |
| | | 1 0 | 5 |

Выводы

Рассмотрены особенности сигнатурного анализа над полем GF(3). Один из подходов компактного анализа - сигнатурно-синдромное тестирование, основанное на операции деления полиномов над полем GF(2) - распространен в область полиномов над полем GF(3). Рассмотрены два варианта применения сигнатурно-синдромного анализатора, построенного на основе полинома над полем GF(3): для локализации ошибочного троичного символа в тестовой реакции и сигнатурно-синдромное тестирование с возможностью аналитического расчета компактных оценок. Полученные результаты могут оказаться полезными при реализации компактного тестирования цифровых устройств.

Литература

1. Дяченко О.Н., Герасимов А.Н. Компактное тестирование на основе многозначной логики // Информатика, кибернетика и вычислительная техника (ИКВТ-97). Сборник научных трудов Донецкого государственного технического университета. Выпуск 1 - Донецкий государственный технический университет. - Донецк, ДонГТУ, 1995. - С.103-110.
2. Дяченко О.Н. Анализ сигнатурной тестируемости комбинационных схем // Автоматика и вычислительная техника. - 1990 - №5. - С.85-89.
3. Дяченко О.Н., Тарасенко А.Н. Спектральный метод компактного тестирования в области сигнатурного анализа // Электрон. моделирование. - 1992. - 14, №6. - С.60-65.
4. Столов Е.Л. Исчерпывающее тестирование программируемых логических матриц и сигнатурный анализ // А и Т. - 1993. - ;№3. - С.160-164.
5. Патент України №6840, G06F 11/00. Сигнатурно-синдромний аналізатор / Дяченко О.М. (Україна); Опубл. 31.03.95. - Бюл. №1.
6. Поспелов Д.А. Логические методы анализа и синтеза схем. - М.: Энергия, 1968.- 228с.