

# ЭФФЕКТИВНОСТЬ КОМПАКТНОГО АНАЛИЗА НАД ПОЛЕМ $GF(3)$

Дяченко О.Н., Солодовников С.В.  
Кафедра ЭВМ ДонГТУ  
don@cs.dgtu.donetsk.ua

## **Abstract**

**Dyachenko O.N., Solodovnikov S.V. Efficiency of compact analysis over field  $GF(3)$ .** The method of analytical calculation of compact estimates is discussed for the case of using characteristic polynomials over  $GF(3)$  for linear feedback shift registers is considered. A simple evaluation of the efficiency of compact testing over  $GF(3)$  is proposed for test generators and analyzers with multiple capacity.

## **Введение**

Увеличение сложности элементов и узлов средств вычислительной техники привело к появлению целого ряда проблем, связанных с задачами тестирования. Среди спектра способов и подходов разрешения или, по крайней мере, облегчения этих задач, важную роль играют методы самотестирования цифровых схем, в частности, методы компактного тестирования. Встроенные средства компактного тестирования применяются в качестве генераторов тестовых последовательностей (ГТП) и анализаторов тестовых реакций (АТР). При сочетании компактного тестирования с методами сканирования, например, методом сквозного сдвигового регистра, задача контроля цифровой схемы сводится к проверке регистров сдвига и комбинационных схем (КС). В этом случае ГТП и АТР для КС реализуются в виде регистров сдвига с линейными обратными связями (РСЛОС) с помощью незначительных изменений регистров сканирования.

В [1-3] выполнен анализ эффективности различных сочетаний порождающих полиномов над полем  $GF(2)$  РСЛОС ГТП и АТР при исчерпывающем тестировании КС. Вместе с тем подобные РСЛОС могут быть реализованы на основе деления полиномов над полем  $GF(3)$ . ГТП в виде РСЛОС с порождающим полиномом над полем  $GF(3)$  (РСЛОС  $GF(3)$ ) генерирует не все возможные двоичные комбинации, т.е. тестирование КС не будет исчерпывающим. В то же время исчерпывающее тестирование КС с большим количеством входов требует значительных временных затрат или в принципе невозможно. Применение ГТП в виде РСЛОС  $GF(3)$  приводит к снижению времени тестирования. При использовании АТР в виде РСЛОС  $GF(3)$  сохраняется возможность анализа эффективности различных сочетаний порождающих полиномов над полем  $GF(3)$  РСЛОС ГТП и АТР.

Данная работа посвящена обобщению результатов анализа эффективности компактного тестирования КС при различных сочетаниях РСЛОС ГТП и АТР [1-3] для порождающих полиномов над полем  $GF(3)$ .

## **1. Аналитический расчет значений сигнатур над полем $GF(3)$ .**

Прежде всего, следует отметить, что анализ эффективности будем рассматривать для КС трехзначной логики при предположении, что наилучшее (наихудшее) сочетание порождающих полиномов над  $GF(3)$  РСЛОС ГТП и АТР будет иметь место для КС как трехзначной, так и двоичной логики.

Функции, описывающие КС трехзначной логики, будем рассматривать в минимизированной сигма – пи нормальной форме. Например, функцию трехзначной логики, заданную таблицей 1, можно представить в следующем виде ( знак "\*" означает умножение по модулю три, знак "+" означает сложение по модулю три ) [4] :

Таблица 1 – Функция трехзначной логики

$V_1 V_2$	$f(V_1, V_2)$	$V_1 V_2$	$f(V_1, V_2)$
0 0	1	1 2	0
0 1	1	2 0	2
0 2	1	2 1	2
1 0	0	2 2	2
1 1	2		

$$\begin{aligned}
 f(V_1, V_2) &= \varphi_0(V_1) * \varphi_0(V_2) + \varphi_0(V_1) * \varphi_1(V_2) + \varphi_0(V_1) * \varphi_2(V_2) + \\
 &+ \varphi_1(V_1) * \varphi_1(V_2) * 2 + \varphi_2(V_1) * \varphi_0(V_2) * 2 + \varphi_2(V_1) * \varphi_1(V_2) * 2 + \\
 &+ \varphi_2(V_1) * \varphi_2(V_2) * 2 = \varphi_0(V_1) + \varphi_1(V_1) * \varphi_1(V_2) * 2 + \varphi_2(V_2) * 2
 \end{aligned}$$

Предположим, что ГТП и АТР реализованы в виде РСЛОС GF(3) с внутренними сумматорами в цепях обратной связи с порождающими полиномами соответственно  $h(x)$  и  $g(x)$ , причем полином  $h(x)$  - примитивный, а корни  $h(x)$  и  $g(x)$  связаны следующим равенством  $b = a^k$ ,  $\deg h(X) = m$ . Если  $m$  равно количеству переменных  $n$ , от которых зависит функция, описывающая КС, то тестирование является псевдо-исчерпывающим, если  $m$  больше  $n$  – тестирование исчерпывающее.

Тестовые наборы, которые поступают на входы исследуемой КС, представляют собой ненулевые элементы поля GF(3<sup>m</sup>), являющимся расширением поля GF(3) над полиномом  $h(x)$ . Эти элементы поля могут быть представлены в троичном, полиномиальном и степенном обозначениях. Каждому ненулевому элементу  $a^k$  поля GF(3<sup>m</sup>) соответствует минимальный полином. Если в качестве порождающего полинома РСЛОС GF(3) АТР выбрать минимальный полином, соответствующий элементу  $a^k$ , то между корнями полиномов  $h(x)$  и  $g(x)$  будет выполнено равенство  $b = a^k$ . В таблице 2 приведены представления элементов поля GF(3<sup>3</sup>) над примитивным полиномом  $h(X) = X^3 + 2X + 1$  в степенном, полиномиальном и троичном обозначениях; каждому ненулевому элементу поставлен в соответствие минимальный полином.

Для полиномов над полем GF(2) минимальные полиномы можно определить из таблицы неприводимых полиномов, представленной в [5]. Для полиномов над полем GF(3) минимальные полиномы для элементов  $a^i$  можно найти аналитически [4].

Анализ эффективности компактного тестирования КС для различных сочетаний порождающих полиномов над полем GF(3) РСЛОС ГТП и АТР, как и в случае GF(2), основан на методе аналитического расчета значений сигнатур. При этом используется только вывод, полученный на основе такого расчета, о равенстве сигнатур нулю в зависимости от ранга конъюнкции КС и числа  $k$ , характеризующего взаимосвязь корней порождающих полиномов.

Прежде всего следует отметить, что конъюнкции трехзначной логики могут иметь коэффициент 2 в качестве множителя. Анализ таблицы 2 показывает, что первая половина ненулевых элементов поля GF(27) в троичном виде ( $a^0, \dots, a^{12}$ ) совпадает со второй половиной ( $a^{13}, \dots, a^{25}$ ) с точностью до обозначений: одна из них может получиться из другой заменой 1(2) соответственно 2(1). Поэтому, сигнатуры текстовых реакций для конъюнкции с коэффициентом 1 и коэффициентом 2 отличаются друг от друга циклическим сдвигом на 13 (в общем случае на  $(3^m - 1)/2$ ).

Таблица 2 – Элементы поля  $GF(3^3)$  и минимальные полиномы.

В виде степени	В виде полинома	В троичном виде	Минимальный полином
0	0	0 0 0	—
$a^0$	1	0 0 1	$Z + 2$
$a^1$	$X$	0 1 0	$Z^3 + 2Z + 1$
$a^2$	$X^2$	1 0 0	$Z^3 + Z^2 + Z + 2$
$a^3$	$X + 2$	0 1 2	$Z^3 + 2Z + 1$
$a^4$	$X^2 + 2X$	1 2 0	$Z^3 + Z^2 + 2$
$a^5$	$2X^2 + X + 2$	2 1 2	$Z^3 + 2Z^2 + Z + 1$
$a^6$	$X^2 + X + 1$	1 1 1	$Z^3 + Z^2 + Z + 2$
$a^7$	$X^2 + 2X + 2$	1 2 2	$Z^3 + Z^2 + 2Z + 1$
$a^8$	$2X^2 + 2$	2 0 2	$Z^3 + 2Z^2 + 2Z + 2$
$a^9$	$X + 1$	0 1 1	$Z^3 + 2Z + 1$
$a^{10}$	$X^2 + X$	1 1 0	$Z^3 + Z^2 + 2$
$a^{11}$	$X^2 + X + 2$	1 1 2	$Z^3 + Z^2 + 2Z + 1$
$a^{12}$	$X^2 + 2$	1 0 2	$Z^3 + Z^2 + 2$
$a^{13}$	2	0 0 2	$Z + 1$
$a^{14}$	$2X$	0 2 0	$Z^3 + 2Z + 2$
$a^{15}$	$2X^2$	2 0 0	$Z^3 + 2Z^2 + Z + 1$
$a^{16}$	$2X + 1$	0 2 1	$Z^3 + 2Z + 2$
$a^{17}$	$2X^2 + X + 2$	2 1 0	$Z^3 + 2Z^2 + 1$
$a^{18}$	$X^2 + 2X + 1$	1 2 1	$Z^3 + Z^2 + Z + 2$
$a^{19}$	$2X^2 + 2X + 2$	2 2 2	$Z^3 + 2Z^2 + Z + 1$
$a^{20}$	$2X^2 + X + 1$	2 1 1	$Z^3 + 2Z^2 + 2Z + 2$
$a^{21}$	$X^2 + 1$	1 0 1	$Z^3 + Z^2 + 2Z + 1$
$a^{22}$	$2X + 2$	0 2 2	$Z^3 + 2Z + 2$
$a^{23}$	$2X^2 + 2X$	2 2 0	$Z^3 + 2Z^2 + 1$
$a^{24}$	$2X^2 + 2X + 1$	2 2 1	$Z^3 + 2Z^2 + 2Z + 2$
$a^{25}$	$2X^2 + 1$	2 0 1	$Z^3 + 2Z^2 + 1$

Следовательно, если сигнатура конъюнкции  $f_1$  с коэффициентом 1 равна нулю, то сигнатура конъюнкции  $f_2$  с коэффициентом 2 также будет равна нулю:  $f_2 = 2 f_1$ ,  $S(f_1) = 0$ , тогда  $S(f_2) = S(2f_1) = 2 S(f_1) = 0$ . Таким образом, для определения зависимости равенства сигнатур нулю от ранга конъюнкции и числа  $-k$ , достаточно вычисления сигнатур конъюнкций с коэффициентом 1.

Для аналитического расчета значений сигнатур воспользуемся методом, аналогичный методу для полиномов над полем  $GF(2)$  [3]. Тестовые наборы будем обозначать в степенном виде. Если  $g(x)$  – примитивный и  $\deg h(x) = \deg g(x) = m$ , тогда 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.

Поскольку в данном случае нас интересует только нулевое значение сигнатур, в дальнейшем будем рассматривать значения сигнатур в обозначениях поля  $GF(3^m)$  над полиномом  $h(x)$ , учитывая, что сигнатура в базисе элементов поля над полиномом  $g(x)$  всегда равна нулю, если она равна нулю в базисе элементов поля над полиномом  $h(x)$ . В этом случае, во-первых, нет необходимости в переходе от значений РСЛОС ГТП к значениям РСЛОС АТР, а, следовательно, в построении матрицы  $M_K$ ; во-вторых, появляется возможность анализа полиномов  $g(x)$  со степенью, меньшей степени  $h(x)$ .

## 2. Анализ эффективности компактного тестирования над полем $GF(3)$ .

Предположим, что  $k = -1$ , т.е. корни полиномов  $h(x)$  и  $g(x)$  связаны равенством  $b = a^{-1}$  или, иными словами,  $h(x)$  и  $g(x)$  – взаимобратные (двойственные) полиномы.

Если ранг конъюнкции равен  $r = m$ , тогда  $S = X^A$ , где  $X^A$  – степенное обозначение тестового набора, на котором функция принимает единичное значение;  $S$  – сигнатура в обозначениях поля  $GF(3^m)$  над полиномом  $h(x)$ .

Если ранг конъюнкции равен  $r = m-1$  и отсутствует переменная  $V_1$ , тогда  $S = X^A + (X^A + 1) + (X^A + 2) = 3X^A + 3 = 0$ . Такой же результат получается и для отсутствующей переменной  $V_2$  :  $S = X^A + (X^A + X) + (X^A + 2X) = 3X^A + 3X = 0$

Предположим, что  $k = -2$ . Если  $r = m$ , тогда  $S = X^{2A}$ .

Если  $r = m-1$  и отсутствует  $V_1$ , тогда

$$S = X^{2A} + (X^A + 1)^2 + (X^A + 2X)^2 = X^{2A} + X^{2A} + 2X^A + 1 + X^{2A} + X^A + 1 = 2$$

$$\text{Если } r = m-1 \text{ и отсутствует } V_2, \text{ тогда } S = X^{2A} + (X^A + X)^2 + (X^A + 2X)^2 = \\ = X^{2A} + X^{2A} + 2X^A X + X + X^2 + X^{2A} + X^A X + X^2 = 2X^2.$$

Следует отметить, что в первом, во втором случаях и при любых других отсутствующих переменных  $V_i$  сигнатуры получаются разными, однако все они не зависят от переменной  $A$ .

Если  $r = m-2$  и отсутствуют  $V_1$  и  $V_2$ , тогда

$$S = (X^A)^2 + (X^A + 1)^2 + (X^A + 2)^2 + (X^A + X)^2 + (X^A + X + 1)^2 + \\ + (X^A + X + 2)^2 + (X^A + 2X)^2 + (X^A + 2X + 1)^2 + (X^A + 2X + 2)^2$$

После раскрытия скобок и преобразований получаем  $S = 0$ . Тот же самый результат получится при любых других отсутствующих двух переменных  $V_i$  и  $V_j$ . Для  $r < m-2$   $S$  также равна 0.

Аналогичным образом можно показать, что сигнатура равна нулю в следующих случаях :  $k = -4, r < m-1$ ;  $k = -5, r < m-1$ ;  $k = -7, r < m-1$ ;  $k = -8, r < m-2$  и т. д.

В общем случае, сигнатура  $S$  принимает ненулевое значение, если ранг конъюнкции  $r < m - [W/2]$ , где  $m$  – число переменных, от которых зависит конъюнкция,  $W$  – вес числа  $-k$ , квадратные скобки означают округление до ближайшего меньшего целого числа.

Учитывая GF(2) и GF(3), можно сделать предположение, что в общем случае для GF(q) справедливо неравенство  $r < m - \lceil W/(q-1) \rceil$ . Таким образом, для РСЛОС GF(3), как и для РСЛОС GF(2), наилучшее сочетание порождающих полиномов ГТП и АТП соответствует  $k = 1$ , т.е. выбору одинаковых полиномов, наихудшее – соответствует  $k = -1$ , т.е. выбору двойственных полиномов, причем в последнем случае, в отличие от GF(2),  $S = 0$  при ранге  $r < m$  ( в поле GF(2)  $S = 0$  при  $r < m-1$  ). Как и в поле GF(2), РСЛОС GF(3) АТП с порождающим полиномом  $Z+2$  занимает особое положение : с одной стороны число  $k = 0$  и его вес равен 0, с другой стороны  $k = 3^m - 1$  и его вес равен  $2m$ . Поэтому сигнатура принимает ненулевое значение при  $r = m$  и  $r < 0$ , т.е. для констант “1” или “2”. Следует отметить, что полином  $Z+1$  соответствует числу  $k = (3^m - 1)/2$  или  $k = -(3^m - 1)/2$ , т.е. является самодвойственным, и имеет вес равный  $m$ .

Итак, если функции  $F$  и  $F'$ , где  $F$  соответствует КС без неисправности,  $F'$  – КС с неисправностью, представленные в сигма - пи нормальной форме, содержат конъюнкции с рангом  $r < m - \lceil W/2 \rceil$ , тогда  $S(F) = 0$  и  $S(F') = 0$  и, следовательно, неисправность будет не обнаружена. Отметим, что в отличие от GF(2), если  $S(F+F') = S(F) + S(F') = 0$  и  $S(F) \neq 0$ , тогда  $S(F) \neq S(F')$ , где знак “+” означает сложение по модулю три.

В таблице 3 представлены примеры формирования сигнатур для ГТП в виде РСЛОС GF(3) с порождающим полиномом  $h(X) = X^3 + 2X + 1$  и двух вариантов порождающих полиномов РСЛОС GF(3) : двойственного  $h'(X) = X^3 + 2X^2 + 1$  и  $h(X) = X^3 + 2X + 1$ .

Таблица 3 – Примеры формирования сигнатур

ГТП h(x)	f	АТП h'(x)	f	АТП h(x)	f <sub>1</sub>	АТП h(x)	f <sub>2</sub>	АТП h(x)	f <sub>3</sub>	АТП h(x)
0 0 1	1	0 0 1	1	0 0 1	1	0 0 1	0	0 0 0	0	0 0 0
0 1 0	0	0 1 0	0	0 1 0	0	0 1 0	0	0 0 0	0	0 0 0
1 0 0	1	1 0 1	1	1 0 1	1	1 0 1	0	0 0 0	0	0 0 0
0 1 2	0	1 1 2	0	0 2 2	0	0 2 2	0	0 0 0	0	0 0 0
1 2 0	2	2 2 1	2	2 2 2	0	2 2 0	2	0 0 2	0	0 0 0
2 1 2	0	1 1 1	0	2 1 1	0	2 2 1	0	0 2 0	0	0 0 0
1 1 1	2	2 1 1	2	1 0 0	0	2 0 1	0	2 0 0	2	0 0 2
1 2 2	2	0 1 0	2	0 1 2	0	0 0 1	2	0 2 1	0	0 2 0
2 0 2	1	1 0 1	1	1 2 1	1	0 1 1	0	2 1 0	0	2 0 0
0 1 1	2	1 1 1	2	2 2 1	0	1 1 0	0	1 2 1	2	0 2 0
1 1 0	0	2 1 2	0	2 0 1	0	1 1 2	0	2 2 2	0	2 0 0
1 1 2	0	0 2 1	0	0 0 1	0	1 0 2	0	2 1 1	0	0 2 1
1 0 2	1	2 1 1	1	0 1 1	1	0 0 0	0	1 0 1	0	2 1 0
0 0 2	1	0 1 2	1	1 1 1	1	0 0 1	0	0 2 2	0	1 2 1
0 2 0	2	1 2 2	2	1 2 1	0	0 1 0	2	2 2 2	0	2 2 2
2 0 0	1	0 2 0	1	2 2 0	1	1 0 1	0	2 1 1	0	2 1 1
0 2 1	2	2 0 2	2	2 2 0	0	0 2 2	2	1 0 0	0	1 0 1
2 1 0	0	2 2 1	0	2 2 1	0	2 2 0	0	0 1 2	0	0 2 2
1 2 1	2	1 1 0	2	2 0 0	0	2 2 1	2	1 2 2	0	2 2 0
2 2 2	2	2 0 1	2	0 2 0	0	2 0 1	2	2 0 1	0	2 2 1
2 1 1	2	2 1 0	2	2 0 2	0	0 0 1	0	0 0 1	2	2 0 0
1 0 1	1	0 0 2	1	0 1 2	1	0 1 1	0	0 1 0	0	0 2 1
0 2 2	2	0 2 2	2	1 2 2	0	1 1 0	2	1 0 2	0	2 1 0
2 2 0	2	2 2 2	2	2 0 1	0	1 1 2	2	0 0 1	0	1 2 1
2 2 1	2	1 2 0	2	0 0 0	0	1 0 2	2	0 1 2	0	2 2 2
2 0 1	1	0 0 0	1	0 0 1	1	0 0 0	0	1 2 0	0	2 1 1

Функция  $f$  соответствует функции, представленной в таблице 1, и содержит конъюнкции с рангом  $r = 2$ . Поэтому при сочетании полиномов ГТП и АТР соответственно :  $h(x)$  и  $h'(x)$   $S(f) = 0$ , поскольку  $r < m - [W/2] = 3$ ;  $h(x)$  и  $h'(x)$   $S(f) \neq 0$ , поскольку  $r \geq m - [W/2] = 1$ . Кроме того, представлены примеры формирования сигнатур конъюнкций  $f_1 = \varphi_0(V_1)$ ,  $f_2 = \varphi_2(V_2) * 2$ ,  $f_3 = \varphi_1(V_1) * \varphi_2(V_2) * 2$ , при этом  $S(f) = S(f_1 + f_2 + f_3) = S(f_1) + S(f_2) + S(f_3)$ . Следует отметить, что  $S(f_1) = 0$ . Этот частный случай подчеркивает тот факт, что даже при выполнении условия  $r \geq m - [W/2]$  сигнатура конъюнкции может принимать нулевое значение, т.е. это условие выражает только необходимое, но не достаточное, условие сигнатурной тестируемости.

Таблица 4 – Функции двоичной логики

$X_1 X_2 X_3 X_4$	$Y_1 Y_2$	$X_1 X_2 X_3 X_4$	$Y_1 Y_2$
0 0 0 0	0 1	0 1 1 0	0 0
0 0 0 1	0 1	1 0 0 0	1 0
0 0 1 0	0 1	1 0 0 1	1 0
0 1 0 0	0 0	1 0 1 0	1 0
0 1 0 1	1 0		

И, наконец, отметим, что рассмотренные в таблице 3 примеры формирования сигнатур могут соответствовать тестированию двухвыходной КС двоичной логики  $Y_1 = X_1 \vee \overline{X_1} X_2 \overline{X_3} X_4$ ;  $Y_2 = \overline{X_1} X_2$ , при предположении, что троичным символам “0”, “1” и “2” соответствуют двоичные “00”, “01” и “10” (см. таблицу 1 и таблицу 4).

## Заключение

Поскольку результаты формирования сигнатур получаются общими для функций двоичной и троичной логики, предположение о наилучшем сочетании порождающих полиномов РСЛОС GF(3) ГТП и АТР, принятое ранее, является верным.

Таким образом, ГТП и АТР в виде РСЛОС GF(3) могут быть использованы для неисчерпывающего тестирования КС двоичной логики, которое имеет актуальное значение при большом количестве входов исследуемой КС. При этом, в отличие от РСЛОС GF(2), можно заранее предсказать, какие двоичные наборы будут присутствовать или отсутствовать в генерируемой тестовой последовательности.

Полученные результаты могут найти применение при реализации самотестирования цифровых схем, проектировании схем встроенного либо внешнего контроля и диагностирования цифровых устройств.

## Литература

1. Ярмолик В.Н., Калоша Е.П. Эффективность сигнатурного анализа в самотестирующихся СБИС // Электронное моделирование. – 1992. – 14, № 3. – с.51–56.
2. Дяченко О.Н. Метод аналитического вычисления сигнатур // Сборник трудов факультета вычислительной техники и информатики.–Выпуск 1. – Донецк : ДонГТУ, 1996. – с.97–102.
3. Дяченко О.Н. Эффективность сигнатурного анализа в цифровых схемах с самотестированием // Электронное моделирование. – 1998. – 20, № 4. – с.79–87.
4. Линейные последовательностные машины. Гилл А., пер. с англ. издательство “Наука”. – Главная редакция физико-математической литературы, М., 1974, 288с.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 594с., ил.