УДК 681.32

О.Н.Дяченко, канд. техн. наук,

(Донецкий государственный технический университет, Донецк)

Эффективность сигнатурного анализа в цифровых схемах с самотестированием

Рассмотрен метод аналитического расчета компактных оценок в случае применения минимальных порождающих полиномов для регистров сдвига с линейными обратными связями. Получена простая оценка эффективности компактного тестирования для генераторов тестовых наборов и анализаторов тестовых реакций кратной разрядности.

The method of analytical calculation of compact estimations in the case of using minimal characteristic polynomials for linear feedback shift registers is considered. A simple evaluation of the compact testing efficiency for test pattern generators and test response analyzers with multiple capacity is suggested.

Розглянуто метод аналітичного розрахунку компактних оцінок у випадку використовування мінімальних породжуючих поліномів для регістрів здвигу з лінейними зворотними зв'язками. Отримана проста оцінка ефективності компактного тестування для генераторів тестових наборів та аналізаторів тестових реакцій кратноі розрядності.

Ключевые слова: компактное тестирование, минимальный полином

Сложность построения тестов для современных БИС и СБИС привела к появлению целого ряда подходов и методов проектирования контролепригодных 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 схем (КС). С помощью незначительных аппаратных затрат сдвиговые регистры легко преобразуются в регистры сдвига с линейными обратными связями (РСЛОС). В результате получаются самотестирующиеся схемы, в которых реализуется компактное тестирование КС. При этом РСЛОС выполняют роль генераторов тестовой последовательности (ГТП) и анализаторов тестовой реакции (АТР).

Применение компактного тестирования ставит задачу определения достоверности результатов тестового эксперимента. Достоверность результатов контроля зависит не только от обнаруживающей смособности того или иного устройства сжатия, но также от распределения вероятностей появления различных выходных реакций, которое, как правило, является неравномерным. Без учета этого обстоятельства применение сигнатурного анализа для некоторых схем может оказаться неэффективным [1]. При исчерпывающем тестировании КС с помощью РСЛОС появляется возможность комплексной оценки достоверности сигнатурного анализа, которая учитывает схемную реализацию РСЛОС ГТП, АТР и конкретные неисправности КС.

В [1-4] предложен метод аналитического расчета сигнатур для РСЛОС ГТП и АТР с примитивными порождающими полиномами одинаковой степени. На основе этого метода получены следующие выводы: различные сочетания порождающих полиномов РСЛОС приводят к разной достоверности сигнатурного анализа; в качестве оценки различных сочетаний порождающих полиномов ГТП и АТР можно использовать количество единиц в двоичном представлении числа $-k$ (вес обратного кода k), где k характеризует взаимосвязь корней полиномов. В частности, максимальная достоверность сигнатурного анализа получается для одинаковых полиномов, минимальная - для взаимообратных. Данная работа посвящена обобщению известных результатов на случай РСЛОС ГТП и АТР с порождающими полиномами кратной степени.

Анализ эффективности компактного тестирования КС с учетом структуры ГТП и АТР выполняется на основе аналитического вычисления компактных оценок. Поэтому прежде всего рассмотрим метод аналитического расчета сигнатур, альтернативный предложенному 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 $b=a^k$, $m=\deg h(X)=\deg g(X)$. Если m равно количеству переменных, от которых зависит булева функция, описывающая КС, то тестирование является исчерпывающим за исключением тестового набора, состоящего из нулей; 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 [5] 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 ненулевых элементов поля $GF(2^5)$ над полиномом $h(X)=X^5+X^2+1$ в степенном, полиномиальном и двоичном обозначениях (для степенного обозначения a^i приведены только показатели степени i). 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 1. Пусть $F_1=\bar{x}_5\bar{x}_4x_3x_2x_1$, $g(X)=X^5+X^3+1$, 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 1. 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 $p=2^m-1$, d- любое целое число. Строка матрицы M_k представляет собой остаток от деления полинома $X^{j/k+(s-1)}$ 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 $X^{0-1}=X^{30}$ на полином $g(X)=X^5+X^3+1$ (см. табл. 1).

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 : 00111. При начальном значении РСЛОС ГТП a^5 значение сигнатуры $S(F_1)=11100$.

Пример 2. Пусть $F_2=\bar{x}_5\bar{x}_4x_3x_2$ при тех же значениях $h(X)$,$g(X)$ и том же начальном состоянии РСЛОС ГТП.

$S(F_2)=M_{-1}X^{19}+M_{-1}(X^{19}+1)=M_{-1}(X^{19}+X^{19}+1)=M_{-1}(00001)=10000.$

Пусть $F_3=\bar{x}_5\bar{x}_4x_3x_1$, $F_4=\bar{x}_4x_3x_2x_1$, $F_5=\bar{x}_5\bar{x}_4x_3$.

$S(F_3)=M_{-1}(X^5+X^5+X)=M_{-1}(X)=M_{-1}(00010)=01000.$

$S(F_4)=M_{-1}(X^{11}+X^{11}+X^4)=M_{-1}(X^4)=M_{-1}(10000)=00001.$

$S(F_5)=M_{-1}(X^2+X^2+1+X^2+X+X^2+X+1)=M_{-1}(0)=0.$

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 [1].

Пример 3. Пусть $F_1=\bar{x}_5\bar{x}_4x_3x_2x_1$, $g(X)=X^5+X^3+X^2+X+1$, 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, $X^{-0/3+(0-1)} = X^{30}$.

Элементу a^1 соответствует полином X^9: $a^1 = a^{1+31*2} = a^{63}$; $X^{-63/3+(0-1)} = X^9$. Аналогично:

$a^2 - X^{19}$: $a^2 = a^{2+31} = a^{33}$; $X^{-33/3+(0-1)} = X^{19}$;

$a^3 - X^{29}$: $a^3 = a^3$; $X^{-3/3+(0-1)} = X^{29}$;

$a^4 - X^8$: $a^4 = a^{4+31*2} = a^{66}$; $X^{-66/3+(0-1)} = X^8$.

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.1):

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

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

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 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 $F=\bar{x}_5\bar{x}_4x_2$: $S(F)=\frac{d}{dz_1}\frac{d}{dz_2}M(0,0,z_2,1,z_1)^3=$

$$=M\frac{d}{dz_1}\frac{d}{dz_2}(z_2z_1;1+z_2;z_2+z;z_1;z_1)=M(10100).$$

Согласно предлагаемому методу расчета сигнатур

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

Следует отметить, что при прежних условиях для $m=6,7,8,\ldots$ 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 $-k$.

Следует отметить, 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 связи с этим при анализе полиномов $g(X)$ со степенью, меньшей степени $h(X)$, значения сигнатур проще рассматривать в обозначениях поля $GF(2^m)$ 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. При этом рассмотренный выше аналитический расчет сигнатур отличается только отсутствием матриц.

Таким образом, несмотря на трудоемкость операций, предлагаемый метод аналитического расчета значений сигнатур позволяет сформулировать важный вывод: при любом начальном состоянии РСЛОС ГТП и РСЛОС ГТП и АТР с порождающими примитивным полиномом $h(X)$ и неприводимым полиномом $g(X)$, корни которых связаны равенством $b=a^k$, $\deg h(X)=m$, $\deg g(X)=n$, значение сигнатуры конъюнкции с рангом $r<m-w$, где w - вес m-разрядного двоичного числа $-k$, равна нулю.

Полученный вывод позволяет распространить оценку эффективности сигнатурного анализа, полученную в [3], для произвольного начального значения РСЛОС ГТП и различных степеней порождающих полиномов : 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 $r<m-w$, то $S(F+F_н)=S(F)+S(F_н)=0$, или $S(F)=S(F_н)$, т.е. неисправность будет необнаруженной.

Практическое значение имеет не столько расчет значений сигнатур, сколько вывод, полученный на основе такого расчета, о равенстве сигнатур нулю в зависимости от ранга конъюнкции КС и веса числа $-k$, характеризующего взаимосвязь корней порождающих полиномов. Это связано с тем, что, чем проще аналитический расчет сигнатур, тем меньше эффективность сигнатурного анализа, и наоборот, при выборе наилучшего сочетания полиномов для обеспечения максимальной эффективности получаем максимальную трудоемкость расчета сигнатур.

Утверждение. Пусть $h(X)$- примитивный полином, $g(X)$- неприводимый полином, $\deg h(X)=m$, $\deg g(X)=n>1$, причем $m/n=z$, z- натуральное число. Тогда вес $w(-k)$ числа $-k$ принимает максимальное значение, равное $m-z$ при

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

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 $GF(2^m)$ [5], 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 равенство (1) с помощью метода математической индукции.

Поскольку z натуральное число, $z>1$. При $z=1$ равенство (1) очевидно.

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

$(2^{(z+1)n}-1)/(2^n-1)=2^{zn}+2^{(z-1)n}+2^{(z-2)n}+\ldots+2^n+1$, 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. Поле $GF(2^n)$ содержит $2^n-1=p$ ненулевых элементов: b^0, ..., b^j, ..., b^{p-1}, количество соответствующих им минимальных полиномов равно 2^n-1. Минимальные полиномы такой же степени соответствуют элементам поля $GF(2^m)$: a^0, ..., a^{jk}, ..., $a^{(p-2)k}$. Поскольку $j<2^n-1$, вес чисел jk, которым соответствуют полиномы степени n, учитывая (1%, равен zw(j), где w(j)- вес числа j в двоичном представлении. Так как w(j)>0, w(k)<w(jk), следовательно, для полиномов degg(X)=n w(k)=z является минимальным.

Итак, $k=(2^m-1)/(2^n-1)$ в двоичном представлении содержит минимальное количество единиц, тогда $-(2^m-1)/(2^n-1)$ содержит максимальное количество единиц. При этом w(-k) принимает минимальное значение. Ч.т.д.

Рассмотрим случай, когда n=1. При этом $k=(2^m-1)=0$, что соответствует полиному g(X)=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.

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 максимальной эффективности сигнатурного анализа 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. 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 [5] расположены на первом месте. Рассмотренный пример показывает, что для разрядности РСЛОС ГТП и АТР соответственно 10 и 5, выбор первых полиномов для 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// Автоматика и вычисл. техника.- 1987.- N 5.- 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. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976.- 594с., ил.

Таблица 1

Представления поля $GF(2^5)$			Состояния РСЛОС АТР	
В виде степени	В виде полинома	В двоичном виде	X^5+X^3+1	$X^5+X^3+X^2+X+1$
1	2	3	4	5
0	0	00000		
a^0	1	00001	00001	00001
a^1	X	00010	00010	00010
a^2	X^2	00100	00100	00100
a^3	X^3	01000	01000	01000
a^4	X^4	10000	10000	10000
a^5	X^2+1	00101	01001	01111
a^6	X^3+X	01010	10010	11110
a^7	X^4+X^2	10100	01101	10011
a^8	X^3+X^2+1	01101	11010	01001
a^9	X^4+X^3+X	11010	11101	10010
a^{10}	X^4+1	10001	10011	01011
a^{11}	X^2+X+1	00111	01111	10110
a^{12}	X^3+X^2+X	01110	11110	00011
a^{13}	$X^4+X^3+X^2$	11100	10101	00110
a^{14}	$X^4+X^3+X^2+1$	11101	00011	01100
a^{15}	$X^4+X^3+X^2+X+1$	11111	00110	11000
a^{16}	X^4+X^3+X+1	11011	01100	11111
a^{17}	X^4+X+1	10011	11000	10001
a^{18}	X+1	00011	11001	01101
a^{19}	X^2+X	00110	11011	11010

Продолжение таблицы 1

1	2	3	4	5
a^{20}	X^3+X^2	01100	11111	11011
a^{21}	X^4+X^3	11000	10111	11001
a^{22}	X^4+X^2+1	10101	00111	11101
a^{23}	X^3+X^2+X+1	01111	01110	10101
a^{24}	$X^4+X^3+X^2+X$	11110	11100	00101
a^{25}	X^4+X^3+1	11001	10001	01010
a^{26}	X^4+X^2+X+1	10111	01011	10100
a^{27}	X^3+X+1	01011	10110	00111
a^{28}	X^4+X^2+X	10110	00101	01110
a^{29}	X^3+1	01001	01010	11100
a^{30}	X^4+X	10010	10100	10111