УДК 681.324 : 621.396

А.Н. Рысованый, В.В. Гоготов

Национальный технический университет "ХПИ", Харьков

ВЫБОР ПОЛИНОМОВ С DEGP(X) = 5 ДЛЯ СИГНАТУРНЫХ АНАЛИЗАТОРОВ В ПОЛЕ ГАЛУА GF(3) ПО КРИТЕРИЮ ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ МАКСИМАЛЬНОЙ ДЛИНЫ

Показан подход к выбору полиномов с degP(x) = 5 для нелинейных регистров сдвига с обратными связями на примере конечного поля Галуа GF(3)

нелинейный регистр сдвига, полином, последовательность максимальной длины

Введение

Постановка проблемы. Классическая стратегия тестирования цифровых схем основана на формировании тестовых последовательностей, позволяющих обнаруживать заданные множества их неисправностей. Для выбора полиномов с последовательностью максимальной длины желательно использовать простейшие методы, позволяющие избежать сложной процедуры их синтеза. К ним относятся следующие алгоритмы:

– формирование всевозможных входных тестовых наборов, т.е. полного перебора двоичных комбинаций. В результате применения подобного алгоритма генерируются счетные последовательности;

– формирование случайных тестовых наборов с требуемыми вероятностями единичного и нулевого символов по каждому входу цифровой схемы;

– формирование псевдослучайных тестовых последовательностей.

Основным свойством распространѐнных алгоритмов формирования тестовых последовательностей является то, что в результате их применения воспроизводятся последовательности двоичных комбинаций очень большой длины. Естественно возникают проблемы их запоминания, передачи и хранения.

Существует достаточно большой класс устройств, при диагностировании которых становится не эффективным двоичный тест. В этом случае целесообразнее применять устройства диагностирования, которые предназначены для решения такого класса задач. Такими устройствами являются нелинейные сигнатурные анализаторы. Однако, при их применении остается нерешенной проблема выбора полиномов, на основании которых выбираются обратные связи. Эти полиномы должны выбираться на основании различных критериев, одним из которых является критерий формирования последовательности максимальной длины. Если же выбирать другие полиномы, то это ведет к уменьшению диагностического теста, и как следствие – к увеличению вероятности необнаружения ошибок.

Таким образом, возникает необходимость в разработке такого подхода к выбору полиномов для конечного поля GF(3), который бы позволял находить полиномы с генерацией последовательности максимальной длины.

Анализ литературы. Цифровые схемы можно тестировать, подавая известные последовательности и контролировать каждый узел при распространении сигнала. При этом цифровые системы радикально отличаются от аналоговых систем не только самой природой сигналов, но и наличием гораздо большего числа сигнальных входов. Один из принципов цифрового тестирования, называемый сигнатурным анализом, описан в [1 – 4]. Кроме того, в [5 – 8] рассмотрены принципы построения и применения сигнатурного анализа. Однако [9, с. 61] «…в настоящее время мы располагаем весьма скудной информацией о построении нелинейных кодеров». Поэтому вопросы выбора полиномов для конечного поля $GP(p^m)$ остается открытым, поскольку ответы на них позволяли бы находить полиномы с генерацией последовательности максимальной длины.

Целью статьи является получение списка полиномов с degP(x) = 5 на примере конечного поля Галуа GF(3) с последовательностями максимальной длины.

Основная часть

На этапе контроля цифровых устройств возникает задача анализа реакций по всем его выходам на подачу на входы по определенному закону тестовых последовательностей. Такое исследование можно осуществить с помощью применения многоканальных сигнатурных анализаторов. Функциональная схема нелинейного сигнатурного анализатора (НСА) с полиномом $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$ приведена на рис. 1.

Коэффициент 1 при степенях полинома указывает на то, что связи вместе со значениями входных

кодов сигналов подключаются на первый регистр через сумматор по модулю 3. Для кодирования трех состояний наиболее часто применяют нулевой, единичный и двоичный элемент наименьшего поля, правила умножения и сложения в котором осуществляются по mod3.

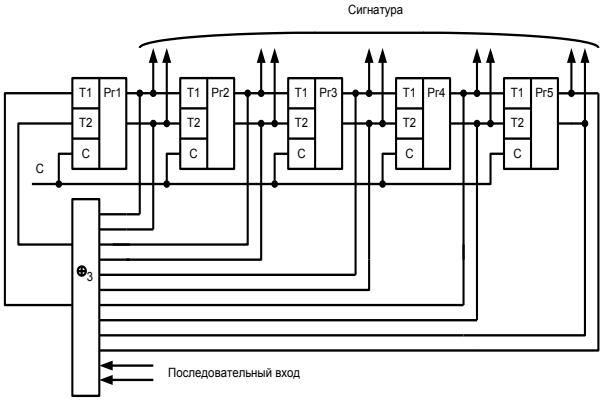

Рис. 1. Функциональная схема НСА с $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$

При подаче на вход НСА с $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$ логической 1 и последующих сдвигах получится матрица состояний H:

1	1	2	1	2	1	1	1	0	2	2	0	2	0	0	1	0	0	1	2
0	1	1	2	1	2	1	1	1	0	2	2	0	2	0	0	1	0	0	1
0	0	1	1	2	1	2	1	1	1	0	2	2	0	2	0	0	1	0	0
0	0	0	1	1	2	1	2	1	1	1	0	2	2	0	2	0	0	1	0
0	0	0	0	1	1	2	1	2	1	1	1	0	2	2	0	2	0	0	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

1	1	2	1	1	0	2	0	1	1	1	2	2	1	1	1	1	0	1	1
2	1	1	2	1	1	0	2	0	1	1	1	2	2	1	1	1	1	0	1
1	2	1	1	2	1	1	0	2	0	1	1	1	2	2	1	1	1	1	0
0	1	2	1	1	2	1	1	0	2	0	1	1	1	2	2	1	1	1	1
0	0	1	2	1	1	2	1	1	0	2	0	1	1	1	2	2	1	1	1
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40

1	1	1	2	0	2	0	2	0	1	2	2	1	0	0	2	2	2	0	0
1	1	1	1	2	0	2	0	2	0	1	2	2	1	0	0	2	2	2	0
1	1	1	1	1	2	0	2	0	2	0	1	2	2	1	0	0	2	2	2
0	1	1	1	1	1	2	0	2	0	2	0	1	2	2	1	0	0	2	2
1	0	1	1	1	1	1	2	0	2	0	2	0	1	2	2	1	0	0	2
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

0	1	0	1	2	1	2	0	0	2	2	0	1	2	1	0	1	2	0	1
0	0	1	0	1	2	1	2	0	0	2	2	0	1	2	1	0	1	2	0
0	0	0	1	0	1	2	1	2	0	0	2	2	0	1	2	1	0	1	2
2	0	0	0	1	0	1	2	1	2	0	0	2	2	0	1	2	1	0	1
2	2	0	0	0	1	0	1	2	1	2	0	0	2	2	0	1	2	1	0
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80

1	2	0	1	2	0	2	2	1	1	0	0	1	0	2	0	0	0	2	1
1	1	2	0	1	2	0	2	2	1	1	0	0	1	0	2	0	0	0	2
0	1	1	2	0	1	2	0	2	2	1	1	0	0	1	0	2	0	0	0
2	0	1	1	2	0	1	2	0	2	2	1	1	0	0	1	0	2	0	0
1	2	0	1	1	2	0	1	2	0	2	2	1	1	0	0	1	0	2	0
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

0	0	0	0
1	0	0	0
2	1	0	0
0	2	1	0
0	0	2	1
101	102	103	104

Для полинома $P(x) = x5 \oplus_3 x4 \oplus_3 x3 \oplus_3 x2 \oplus_3 x \oplus_3 1$ число состояний $l = 104$.

Исходное состояние любого НСА, как и линейного СА, должно быть $h1 = \|10000\|$. Однако, при значении коэффициента при x равного 2 исходное состояние формируется с выхода первого триггера, и будет иметь вид $h1 = \|20000\|$.

В общем случае матрица состояний имеет вид:

$$H = \|h_1 h_2 h_3 \ldots h_i \ldots h_n\|^T,$$

где $h_1 = \|10000\|$ либо $h_1 = \|20000\|$;

T – символ транспонирования матрицы.

Для полинома $P(x) = x5 \oplus_3 x4 \oplus_3 x3 \oplus_3 x2 \oplus_3 x \oplus_3 1$ n-е (104-е) состояние регистра $hn = \|00001\|$. При осуществлении еще одного сдвига получим:

$$h_{n+1} = h_1,$$

т.е. состояния регистра повторяются.

Число состояний l при degP(x)= 5 в поле GF(3) равно:

$$l = 3^n - 1 = 242.$$

Следовательно, к полиномам максимальной (M) длины при degP(x)= 5 в конечном поле GF(3) необходимо относить полиномы, которые генерируют число своих состояний l = 242. На практике, это означает перебор всех состояний из трех (0, 1, 2).

Выбор обратных связей в схеме осуществляется в соответствии со степенями полинома, имеющими ненулевые значения. Эти связи вместе со значениями входных кодов сигналов подключаются на первый регистр через сумматор по модулю 3.

Одним из наиболее распространѐнных в настоящее время методов формирования последовательностей является преобразование сигналов, получаемых с помощью так называемых генераторов белого шума (ГБШ). В применении к цифровым методам генерирования под белым шумом понимается последовательность некоррелированных чисел или цифр, распределѐнных, как правило, по равномерному закону.

Известны два основных метода получения цифрового белого шума: физический - генерирование случайных двоичных чисел с помощью специальных устройств - генераторов случайных чисел (ГСЧ); математический - формирование псевдослучайных числовых последовательностей (ПСЧП) по специальным программам или с использованием генераторов псевдослучайных чисел (ГПСЧ).

Ниже приведен фрагмент программы, который позволяет генерировать последовательности:

```
// Запоминание текущего состояния регистров
a1:=t[1];
b1:=t[2];
c1:=t[3];
d1:=t[4];
e1:=t[5];
// Вычисление нового состояния регистров
t[5]:=(a2*t[4]) mod 3;
if b2<>2 then  t[4]:=(t[3]) mod 3 else
t[4]:=(2*t[3]) mod 3;
if c2<>2 then  t[3]:=(t[2]) mod 3 else
t[3]:=(2*t[2]) mod 3;
if d2<>2 then t[2]:=(t[1]) mod 3 else
t[2]:=(2*t[1]) mod 3;
// Вычисление исходного состояния
if e2<>2 then
t[1]:=(k5*a1+k4*b1+k3*c1+k2*d1+k1*e1) mod 3 else
t[1]:=(2*(k5*a1+k4*b1+k3*c1+k2*d1+k1*e1)) mod 3;
// Вычисление длины последовательности
n:=n+1;
```

где a1, b1, c1, d1, e1 используется как буфер;
t[1-5] – текущее состояние регистров;
k[1-5] – признак наличия обратных связей.

Результатом выполнения программы, являются полиномы с $degP(x) = 5$ с формированием последовательности максимальной длины $l = 242$:

P(x) = x5 ⊕3 x3 ⊕3 2x ⊕3 1;
P(x) = x5 ⊕3 2x3 ⊕3 x2 ⊕3 1;
P(x) = x5 ⊕3 2x3 ⊕3 x2 ⊕3 x ⊕3 1;
P(x) = x5 ⊕3 x4 ⊕3 x2 ⊕3 2x ⊕3 1;
P(x) = x5 ⊕3 x4 ⊕3 2x2 ⊕3 1;
P(x) = x5 ⊕3 x4 ⊕3 x3 ⊕3 2x ⊕3 1;
P(x) = x5 ⊕3 x4 ⊕3 x3 ⊕3 2x2 ⊕3 x ⊕3 1;
P(x) = x5 ⊕3 x4 ⊕3 2x3 ⊕3 2x2 ⊕3 2x ⊕3 1;
P(x) = x5 ⊕3 2x4 ⊕3 x ⊕3 1;
P(x) = x5 ⊕3 2x4 ⊕3 x3 ⊕3 1;
P(x) = x5 ⊕3 2x4 ⊕3 x3 ⊕3 x2 ⊕3 1;
P(x) = x5 ⊕3 2x4 ⊕3 2x3 ⊕3 x2 ⊕3 2x ⊕3 1;
P(x) = 2x5 ⊕3 x ⊕3 1;
P(x) = 2x5 ⊕3 2x2 ⊕3 2x ⊕3 1;
P(x) = 2x5 ⊕3 x3 ⊕3 2x2 ⊕3 2x ⊕3 1;
P(x) = 2x5 ⊕3 2x3 ⊕3 2x2 ⊕3 1;
P(x) = 2x5 ⊕3 x4 ⊕3 1;
P(x) = 2x5 ⊕3 x4 ⊕3 x2 ⊕3 x ⊕3 1;
P(x) = 2x5 ⊕3 x4 ⊕3 x3 ⊕3 x ⊕3 1;
P(x) = 2x5 ⊕3 x4 ⊕3 2x3 ⊕3 2x2 ⊕3 1;
P(x) = 2x5 ⊕3 2x4 ⊕3 2x ⊕3 1;
P(x) = 2x5 ⊕3 2x4 ⊕3 x3 ⊕3 x2 ⊕3 2x ⊕3 1.

Сигнатурный анализ представляет собой простой способ тестирования, заключающийся в проверке отдельных узлов схемы и сравнения их сигнатур с документированными значениями. Применение сигнатурного анализатора позволяет быстро идентифицировать неисправность в системе, а затем локализовать неисправный компонент. Любые модификации в системе влекут за собой необходимость повторного получения всех сигнатур в системе, поэтому при ее модификациях и усовершенствованиях необходимо составлять скорректированные таблицы сигнатур.

Выводы

В результате исследований был получен полный список полиномов с degP(x) = 5 для конечного поля Галуа GF(3). Установлено, что количество полиномов с последовательностью максимальной длины равной 242 не превысило числа 22.

Выяснено, что на исходное состояние НСА влияет значение коэффициента, отличного от нуля при аргументе с младшей степенью.

Список литературы

1. Кирьянов К.Г., Соловейчик Э.Б. К проектированию РЭА, ориентированной на диагностику сигнатурным анализом // Техника средств связи. Сер. Радиоизмерительная техника. – 1980. – Вып. 1 (26). – С. 9-84.

2. Пухальский Г.И., Новосельцева Т.Я. Цифровые устройства: Учебное пособие для втузов. – СПб.: Политехника, 1996.

3. Основы сигнатурного анализа ЭВМ и вычислительных систем. Учебное пособие. А.Н. Рысованый и др. Х.: ХВУ, 1996. – 42 с.

4. Барашко А. С. Об одной гипотезе, касающейся нелинейных аналогов примитивных сигнатурных анализаторов // Электронное моделирование. – 2000. – Т. 22. – №6. – С. 84-89.

5. Основи теорії синтезу сигнатурних аналізаторів. Навчальний посібник / За ред. О.М.Рисованого. – Харків: ХВУ, 1998. – 122 с.

6. Латыпов Р.Х. Воспроизведение тестовых наборов и сжатие данных нелинейными регистрами сдвига // Автоматика и телемеханика. – М.: Наука. – 1989. – № 10. – С. 167-172.

7. Барашко А. С. Характеристическая функция нелинейного сигнатурного анализатора // Электронное моделирование. – 2000. – Т.22. – №6. – С. 59-65.

8. Науменко М.І., Стасєв Ю.В., Кузнєцов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Х.: ХУПС, 2005. – 267 с.

9. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.

Поступила в редколлегию 6.04.2007

Рецензент: д-р техн. наук проф. И.И. Обод, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.