УДК 004.272.43

А.Н. РЫСОВАНЫЙ, канд. техн. наук, НТУ "ХПИ",
В.В. ГОГОТОВ, НТУ "ХПИ"

ВЫБОР ПОЛИНОМОВ ДЛЯ СИГНАТУРНЫХ АНАЛИЗАТОРОВ В ПОЛЕ ГАЛУА *GF*(3) ПО КРИТЕРИЮ СЛОЖНОСТИ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ

Показаний підхід до вибору поліномів з $degP(x) = 4$ для регістрів із зворотними зв'язками по критерію складності технічної реалізації на основі повного списку поліномів для кінцевого поля Галуа $GF(3)$.

Approach is shown to the choice of polynomials with $degP(x) = 4$ for registers with feed-backs on the criterion of complication of technical realization on the basis of complete list of polynomials for the eventual field of Galua of GF(3).

Постановка проблемы. Широкое распространение радиоэлектронных устройств с применением цифровой обработки сигналов обуславливает повышенный интерес к вопросам диагностирования их технического состояния.

Одной из разновидностей диагностирования цифровых узлов и блоков является тестовое диагностирование, применение которого на этапе проектирования и изготовления цифровых узлов позволяет определить правильность их функционирования и осуществить процедуру поиска неисправностей. При разработке тестовой диагностики возникает сложность в определении эталонных реакций при тестировании существующих схем, в определении оптимального числа контрольных точек для снятия выходной реакции диагностируемой цифровой схемы. Это можно сделать, либо создавая прототип разрабатываемого цифрового устройства и проводя его диагностику аппаратными методами, либо осуществляя моделирование на персональном компьютере как цифрового устройства, так и процесса диагностики. Наиболее рациональным является второй подход, который предполагает создание автоматизированных систем диагностики, позволяющих производить диагностику цифровых схем на стадии проектирования. Наибольший интерес представляют системы диагностики с использованием нелинейных регистров сдвига с обратными связями [1 – 4], вопросы синтеза и применения которых нуждаются в дальнейших совершенствованиях.

До настоящего времени не существовало полного списка полиномов для конечного поля Галуа $GF(3)$, которые обладали бы определенными обнаруживающими способностями и возможностью определять классы ошибок в зависимости от длины исследуемой последовательности.

Таким образом, возникает необходимость в разработке методики выбора полиномов для конечного поля $GP(p^m)$, которая бы позволяла находить полиномы с генерацией последовательности максимальной длины.

Анализ литературы. Регистры сдвига с обратными связями находят широкое применение при построении тестовых генераторов [5, 6], при этом, наиболее простой путь заключается в построении линейных регистров сдвига с обратными связями [7, 8]. Однако [9, с. 61] "… в настоящее время мы располагаем весьма скудной информацией о построении нелинейных кодеров". В работе [10, с. 3] речь идет о том, что "… разрыв между практикой и математической теорией недвоичного помехоустойчивого кодирования не сокращается или сокращается недостаточно быстрыми темпами". Общие принципы построения и применения сигнатурного анализа приводятся в работе [11]. Однако, в этих работах не рассматриваются вопросы выбора полиномов для конечного поля $GP(p^m)$, ответы на которые позволяли бы находить полиномы с генерацией последовательности максимальной длины, а в дальнейшем, и определять полиномы с определенным классом обнаруживаемых ошибок.

Целью статьи является получение полного списка полиномов на примере конечного поля Галуа $GF(3)$ с анализом длин последовательностей.

Основная часть. Современные цифровые устройства, как правило, являются многовыходными. Поэтому на этапе их контроля возникает задача анализа реакций по всем выходам цифрового устройства на подачу на входы по определенному закону тестовых последовательностей. Такое исследование можно осуществить с помощью применения многоканальных сигнатурных анализаторов.

Математическая запись полиномов для регистров сдвига имеет вид: $P(x) = a_0x^n \oplus_k a_1x^{n-1} \oplus_k \ldots \oplus_k a_n$, где при $k = 2$ выполняется сложение по mod2. Если коэффициент при нулевой степени аргумента $a_n = 1$, то такой полином называется характеристическим. Для нелинейных регистров сдвига с обратными связями для конечного поля Галуа $GF(3)$ a_n, $a_0 \in \{1, 2\}$, $a_i \in \{0, 1, 2\}$ при $i = \overline{1, n-1}$. Таким образом, нелинейные регистры сдвига с обратными связями могут и не быть характеристическими.

Функциональная схема одноканального нелинейного сигнатурного анализатора с полиномом $P(x) = x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$ приведена на рис.

В общем случае число состояний l для конечного поля $GP(p^m)$ будет определяться выражением:

$$l = p^m - 1. \qquad (1)$$

Таким образом, число состояний l при $degP(x) = 4$ в поле $GF(3)$ равно:

$$l = 3^n - 1 = 80.$$

Следовательно, к полиномам максимальной длины при $degP(x) = 4$ в конечном поле $GF(3)$ необходимо относить полиномы, которые генерируют число своих состояний $l = 80$.

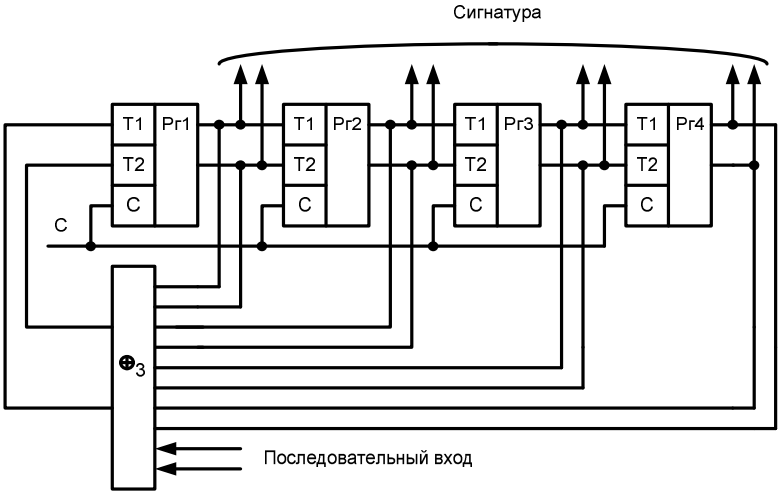

Рис. Функциональная схема

Если на вход нелинейного сигнатурного анализатора, описанного многочленом $P(x) = x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$, подать логическую 1, а потом производить сдвиги, то получится следующая матрица состояний H:

1	1	2	1	2	0	2	2	0	1	2	2	2	1	1	0	1	0	2	0	0	2	1	0	0	0
0	1	1	2	1	2	0	2	2	0	1	2	2	2	1	1	0	1	0	1	0	0	2	1	0	0
0	0	1	1	2	1	2	0	2	2	0	1	2	2	2	1	1	0	1	0	2	0	0	2	1	0
0	0	0	1	1	2	1	2	0	2	2	0	1	2	2	2	1	1	0	1	0	2	0	0	2	1
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**

Полный список полиномов на примере поля Галуа *GF*(3) с анализом длин последовательностей можно получить с помощью программы, реализованной по алгоритму:

1. Перебор весовых коэффициентов: для старшего и свободного от 1 до 2, для остальных от 0 до 2.
2. Установка флага окончания генерирования последовательностей.
3. Подача входного сигнала.
4. Проверка существования обратных связей.
5. Вывод на экран последовательности с увеличением содержимого счетчика длины генерируемых последовательностей.
6. Запоминание текущего состояния регистров.
7. Проверка на весовые коэффициенты.
8. Вычисление нового состояния регистров.

Результатом выполнения программы, которая использует алгоритм, являются полиномы с $degP(x) = 4$ с указанием длин последовательностей l:

$l = 80$: $x^4 \oplus_3 x \oplus_3 1$;	$2x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;	$x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 1$;
$x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;	$2x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 1$;
$2x^4 \oplus_3 2x \oplus_3 1$;	$l = 20$: $x^4 \oplus_3 2x^3 \oplus_3 x \oplus_3 1$;
$2x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;	$2x^4 \oplus_3 2x^3 \oplus_3 2x \oplus_3 1$;
$2x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;	$l = 18$: $x^4 \oplus_3 x^3 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 x^3 \oplus_3 1$;	$l = 16$: $x^4 \oplus_3 x^2 \oplus_3 1$;
$2x^4 \oplus_3 2x^3 \oplus_3 1$;	$2x^4 \oplus_3 2x^2 \oplus_3 1$;
$l = 40$: $x^4 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;	$l = 13$: $x^4 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;	$2x^4 \oplus_3 x^2 \oplus_3 x \oplus_3 1$;
$x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 1$;	$x^4 \oplus_3 2x^3 \oplus_3 1$;
$2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 1$;	$2x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 1$;
$l = 26$: $x^4 \oplus_3 x^2 \oplus_3 x \oplus_3 1$;	$l = 12$: $x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;	$2x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$;
$x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$;	$2x^4 \oplus_3 x^2 \oplus_3 1$;
$x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;	$l = 10$: $2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;
$2x^4 \oplus_3 x \oplus_3 1$;	$l = 9$: $2x^4 \oplus_3 x^3 \oplus_3 x \oplus_3 1$;
$2x^4 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;	$l = 8$: $x^4 \oplus_3 x^3 \oplus_3 x \oplus_3 1$;
$2x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;	$x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;
$2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 2x \oplus_3 1$;	$2x^4 \oplus_3 x^3 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 1$;	$2x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;
$x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 1$;	$2x^4 \oplus_3 1$;
$2x^4 \oplus_3 x^3 \oplus_3 1$;	$l = 6$: $x^4 \oplus_3 2x^3 \oplus_3 2x \oplus_3 1$;
$2x^4 \oplus_3 x^3 \oplus_3 2x^2 \oplus_3 1$;	$2x^4 \oplus_3 2x^3 \oplus_3 x \oplus_3 1$;
$l = 24$: $x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$;	$x^4 \oplus_3 2x^2 \oplus_3 1$;
$2x^4 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;	$l = 5$: $x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 2x \oplus_3 1$;
$2x^4 \oplus_3 2x^2 \oplus_3 x \oplus_3 1$;	$l = 4$: $x^4 \oplus_3 1$.

Полученные полиномы генерируют последовательности с длинами от $l = 4$ до $l = 80$.

Выводы. В результате исследований был получен полный список полиномов с $degP(x) = 4$ для конечного поля Галуа $GF(3)$. Установлено, что количество полиномов с последовательностью максимальной длины, равной 80, не равно восьми. Выяснено, что значение свободного коэффициента a_n при x^n (кроме $a_n \neq 0$) не влияет на длину генерируемой последовательности, а последовательности при $a_n = 1$ и $a_n = 2$ повторяют друг друга. Также было установлено, что на сложность технической реализации существенно влияет только количество входов сумматоров по модулю выбранного полинома.

Список литературы: 1. *Латыпов Р.Х.* Воспроизведение тестовых наборов и сжатие данных нелинейными регистрами сдвига // Автоматика и телемеханика. – М.: Наука. – 1989. – № 10. – С. 167 – 172. **2.** *Барашко А.С.* Характеристическая функция нелинейного сигнатурного анализатора // Электронное моделирование. – 2000. – Т. 22. – № 6. – С. 59 – 65. **3.** *Барашко А.С.* Об одной гипотезе, касающейся нелинейных аналогов примитивных сигнатурных анализаторов // Электронное моделирование. – 2000. – Т. 22. – № 6. – С. 84 – 89. **4.** *Рысованый А.Н., Гоготов В.В.* Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины // Системи управління, навігації та зв'язку. – К.: Центральний науково-дослідний інститут навігації і управління, 2007. – Вип.1.– С. 77 – 79. **5.** *Питерсон У.* Коды, исправляющие ошибки. – М.: Мир, 1976. – 594 с. **6.** *Науменко М.І., Стасєв Ю.В., Кузнєцов О.О.* Теоретичні основи та методи побудови алгебраїчних блокових кодів. – Х.: ХУПС, 2005. – 267 с. **7.** Основи теорії синтезу сигнатурних аналізаторів. Навчальний посібник / За ред. *О.М. Рисованого.* – Харків: ХВУ, 1998. – 122 с. **8.** *Тупкало В.Н.* Основы теории сигнатурного контроля цифровых систем. – К.: МО Украины, 2004. – 324 с. **9.** *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с. **10.** *Муттер В.М.* Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 288 с. **11.** *Ярмолик В.Н.* Контроль и диагностика цифровых узлов ЭВМ. – Мн.: Наука и техника, 1988. – 240 с.

Поступила в редакцию 11.04.2007