УДК 004.272.43

В.В. ГОГОТОВ, аспирант НТУ "ХПИ"

ОПРЕДЕЛЕНИЕ ПЕРИОДИЧЕСКОЙ СТРУКТУРЫ ПОСЛЕДОВАТЕЛЬНОСТИ, ПОРОЖДАЕМОЙ МНОГОЧЛЕНОМ С МИНИМАЛЬНЫМ ЭЛЕМЕНТОМ РАЗЛОЖЕНИЯ

Проведен анализ влияния минимального элемента разложения в структуре разложения на длину генерируемой последовательности. Определена периодическая структура последовательности, порождаемой многочленом с минимальным элементом разложения. Получена математическая зависимость, позволяющая определять длину формируемой последовательности по виду разложения.

Ключевые слова: многочлен с минимальным элементом разложения, периодическая структура, длина формируемой последовательности.

Постановка проблемы и анализ литературы. В настоящее время известны несколько областей, где случайные и псевдослучайные числа широко используются в процессе решения задач. К таким областям относятся статистическое моделирование, системы передачи информации, идентификация объектов управления, вероятностное тестирование, защита информации в сетях и другие.

Для решения этих задач необходимо вырабатывать "несметные количества случайных чисел с самыми разнообразными свойствами" [1, 2]. По сообщению японских учёных, "согласно статистическим данным, среди используемых подпрограмм математической библиотеки большого ВЦ Токийского университета, подпрограммы генерации равномерно распределённых случайных чисел в последнее время находятся в группе самого высокого ранга использования" [3]. Наибольшее значение для практики имеют числа с равномерным законом распределения. Одними из основных элементов в таких системах являются генераторы псевдослучайных последовательностей, от качества и быстродействия которых существенно зависят результаты решения поставленных задач.

Известны фундаментальные работы в области генерирования псевдослучайных последовательностей и чисел, а также большое количество патентов и авторских свидетельств, которые говорят о большом интересе к этим областям. Решению таких задач посвящены работы ученых: Иванова М.А., Клейнена Д., Кузнецова В.М., Гришкина С.Г., Морозова А.М., Корна Г., Орлова М.А., Чугункова И.В., Яковлева В.В., Ярмолика В.Н. и других.

Однако влияние минимального элемента разложения ($x \oplus_3 1$) в структуре разложения на длину генерируемой последовательности изучено еще не достаточно.

В отечественной и зарубежной литературе основное внимание при формировании псевдослучайных чисел уделено генераторам псевдослучайных последовательностей, построенных на основе регистра сдвига с линейной обратной связью (с сумматорами по модулю два), причем в большинстве работ рассматриваются последовательности максимальной длины. Г. Корн в работе [4] рассматривает цифровой метод формирования шума при разработке аналоговой машины ASTRAC II в Аризонском университете (США), предназначенной для статистической обработки реализаций случайных процессов. Генератор двоичной последовательности состоит из 25-разрядного сдвигового регистра и одного сумматора по модулю 2. В работе [5] приводится пример сочетания цифровых и аналоговых методов при формировании аналогового сигнала в виде белого шума. В [6 – 13] рассмотрены свойства и особенности последовательностей максимальной длины, показан подход к построению генераторов псевдослучайных последовательностей, получения матриц состояний. Основные свойства и структурные особенности последовательностей максимальной длины также описаны в [14, 15]. Однако [16] "значительная часть установленных здесь фактов – не доказанные теоремы, а эмпирические наблюдения, ожидающие смелых исследователей".

Поэтому исследование периодических структур и статистических характеристик последовательностей, формируемых генераторами псевдослучайных последовательностей на основе регистра сдвига с сумматорами по модулю три, является актуальной задачей, имеющей существенное значение для статистического моделирования.

Целью статьи является получение периодической структуры последовательности, порождаемой многочленом $f(x) = (x \oplus_3 1) f_2(x)$.

Основная часть. Многочлен $f(x)$ степени N с коэффициентами из $GF(3)$ называется неприводимым, если он не делится ни на один другой многочлен степени меньшей N и большей 0. Многочлен $f(x)$ степени N с коэффициентами из $GF(3)$ называется примитивным, если он не делит нацело ни один многочлен вида $x^S - 1$, где $S < L^N - 1$.

Периодическую структуру последовательностей в общем случае представляют в виде:

$$\left[\mu_1(L_1),\ \mu_2(L_2),\ \ldots,\ \mu_i(L_i)\right], \qquad (1)$$

где L_i – длина i-го периода, μ_i – количество периодов длиной L_i.

Известно, что если многочлен $f(x)$ степени N с коэффициентами из $GF(3)$ неприводим и примитивен, то периодическая структура линейно-рекуррентной последовательности имеет вид $[1(1),\ 1(3^n - 1)]$. При этом на всех выходах регистра формируются последовательности n-го порядка, а запрещенным является состояние (0 0 … 0).

Функциональная схема генератора псевдослучайных последовательностей на регистрах сдвига с обратной связью, который описывается полиномом $f(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$, приведена на рисунке.

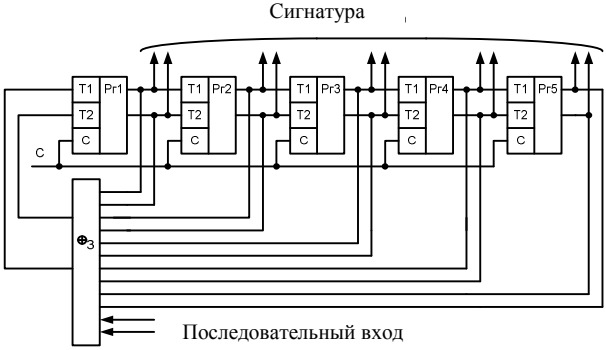

Рис. Функциональная схема генератора псевдослучайных последовательностей на регистрах сдвига с обратной связью с $f(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$

Работа генератора псевдослучайных последовательностей на регистрах сдвига с обратной связью описывается с помощью матрицы состояний, которая для схемы рис. имеет следующий вид:

1121211102202001001211211020111221111011111202020122100222000101212002201210120112012022110010200021000
0112121110220200100121121102011122111101111120202012210022200010121200220121012011201202211001020002100
0011212111022020010012112110201112211110111112020201221002220001012120022012101201120120221100102000210
0001121211102202001001211211020111221110111111202020122100222000101212002201210120112012022110010200210
0000112121110220200100121121102011122111101111202020122100222000101212002201210120112012022110010200021

Особенность в периодическую структуру линейно-рекуррентной последовательности вносит множитель ($x \oplus_3 1$). Поэтому рассмотрим недостаточно исследованные и наиболее интересные для практики случаи, когда многочлен $f(x)$ имеет вид:

$$f(x) = \left[f_1(x)\right]^i \cdot f_2(x) \cdot \ldots \cdot f_r(x), \qquad (2)$$

где $f_j(x)$, $j = \overline{2, r}$ – неприводимые многочлены степени n_j, $f_1(x) = (x \oplus_3 1)$, $\sum_{j=2}^{r} n_j + i = n$.

Каждому сомножителю $f_j(x)$ как неприводимому многочлену соответствует свой период L_i. При $n_i > 1$ период L_i не обязательно будет максимальным и равным, поскольку $f_j(x)$ может быть не примитивным.

Символически периодическая структура соответствующей последовательности записывается в виде $[1(1),\mu_i(L_i)]$. В этом случае периодическая структура, соответствующая многочлену (2), представляет собой совокупность простых и комбинационных периодов и определяется как формальное произведение членов $[1(1)+\mu_i(L_i)]$. В случае, если

$$f(x) = f_i(x) \cdot f_j(x) \tag{3}$$

и $f_i(x)$ и $f_j(x)$ имеют периодические структуры $[1(1),\mu_i(L_i)]$ и $[1(1),\mu_j(L_j)]$ соответственно, то периодическая структура, соответствующая многочлену (3), определяется как:

$$[1(1)+\mu_i(L_i)]\cdot[1(1)+\mu_j(L_j)] = 1(1)+\mu_i(L_i)+\mu_j(L_j)+\mu_{ij}(L_{ij}), \tag{4}$$

где L_{ij} – наименьшее общее кратное L_i и L_j, а $\mu_{ij} = \mu_i\mu_j(L_i, L_j)$, где ($L_i$, L_j) – наибольший общий делитель L_i и L_j.

Рассмотрим случай, когда многочлен $f(x)$ в выражении (2) имеет вид:

$$f(x) = (x \oplus_3 1) f_2(x), \tag{5}$$

где многочлен $f_2(x)$ степени $(n-1) \geq 3$ неприводим и примитивен.

При многочлене $(x \oplus_3 1)$ периодическая структура последовательности имеет вид $[1(3)]$. Тогда определим периодическую структуру последовательности, порождаемой многочленом (5):

$$[1(3)]\cdot[1(1)+1(3^{n-1}-1)] = 1(3)+1(3^{n-1}-3). \tag{6}$$

Многочлен $f(x) = x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$ в выражении (2) имеет вид: $f(x) = (x \oplus_3 1)(x^3 \oplus_3 x^2 \oplus_3 1)$.

Матрица состояний для многочлена $f(x) = x^4 \oplus_3 2x^3 \oplus_3 x^2 \oplus_3 x \oplus_3 1$ имеет вид:

11222122100022111211200
01122212210002211121120
00221112112000112221210
00022111211200011222122

Для заданного многочлена длина формируемой последовательности равна $l = 24$.

Воспользовавшись (6), рассчитаем длину формируемой генератором последовательности, которая описывается многочленом третьей степени: $3^{n-1} - 3 = 3^{4-1} - 3 = 3^3 - 3 = 27 - 3 = 24$.

Как видно из расчетов, результаты, полученные с помощью соотношения (6), и с помощью построенной матрицы состояний для заданного многочлена третьей степени полностью совпали.

Многочлен $f(x) = x^5 \oplus_3 2x^4 \oplus_3 x^3 \oplus_3 x \oplus_3 1$ в форме (2) имеет вид: $f(x) = (x \oplus_3 1)(x^4 \oplus_3 x^3 \oplus_3 1)$.

Матрица состояний для многочлена $f(x) = x^5 \oplus_3 2x^4 \oplus_3 x^3 \oplus_3 x \oplus_3 1$ имеет вид:

```
111221100121201002102112122021002210000222112200212102001201221211012001120000
011122110012120100210211212202100221000022211220021210200120122121101200112000
001112211001212010021021121220210022100002221122002121020012012212110120011200
000222112200212102001201221211012001120000111221100121201002102112122021002210
000022211220021210200120122121101200112000011122110012120100210211212202100221
```

Для заданного многочлена длина формируемой последовательности равна $l = 78$.

Воспользовавшись (6), рассчитаем длину формируемой генератором последовательности, которая описывается многочленом четвертой степени:
$3^{n-1} - 3 = 3^{5-1} - 3 = 3^4 - 3 = 81 - 3 = 78$.

Как видно из расчетов, результаты, полученные с помощью соотношения (6), и с помощью построенной матрицы состояний для заданного многочлена четвертой степени полностью совпали.

Выводы. В результате исследования была получена математическая зависимость, позволяющая определять длину формируемой последовательности по виду разложения. Определена периодическая структура последовательности, позволяющая рассчитать длину матрицы состояний. Результаты исследования позволят разработать методику синтеза генераторов псевдослучайных последовательностей на основе регистров сдвига с сумматорами по модулю три.

Список литературы: **1.** *Иванова В.М.* Случайные числа и их применение. – М.: Финансы и статистика, 1984. – 111 с. **2.** *Клейнен Д.* Статистические методы в имитационном моделировании. – М.: Статистика, 1978. – 221 с. **3.** *Fushimi Masanori.* Методы генерации псевдослучайных чисел: Дзехо серес // ВЦП. – 1980. – № Г-32668. – Vol. 21. – № 9. – P. 968 – 974. **4.** *Корн Г.* Моделирование случайных процессов на аналоговых и аналогово-цифровых машинах. – М.: Мир, 1968. – 315 с. **5.** *Хоровиц П., Хилл У.* Искусство схемотехники. В 2-х томах. – Т. 2. – М.: Мир, 1983. – 590 с. **6.** *Иванов М.А., Чугунков И.В.* Теория, применение и оценка генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с. **7.** *Зензин О.С., Иванов М.А.* Стандарт криптографической защиты XXI века – AES. Теория конечных полей / Под ред. М.А. Иванова. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с. **8**. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. – М.: Мир, 1976. **9.** *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. **10.** *Рысованый А.Н., Гоготов В.В.* Методика построения нелинейного генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3 // Інформаційно-керуючи системи на залізничному транспорті, 2008. – Вип. № 5 – 6. – С. 21 – 25. **11.** *Рысованый А.Н., Гоготов В.В.* Выбор полиномов с $DEGP(x) = 5$ для сигнатурных анализаторов в поле Галуа $GF(3)$ по критерию формирования последовательности максимальной длины // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2007. – Вип. 2 (14). – С. 126 – 128. **12.** *Макуильямс Ф. Дж., Слоан Н. Дж. А.* Псевдослучайные

последовательности и таблицы // ТИИЭР. – 1976. – № 12. – С. 80–95. **13.** *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с. **14.** *Arvillias A.C., Maritsas D.G.* Toggle-Registers Generating in Parallel k^{th} Decimaitions of m-Sequences xp + xk + 1 Design Tables // IEEE Transaction on Computers. V. C-28. – 1979. – № 2. – P. 89-100. **15.** *Pradhan D.K., Hsiao M.Y., Patel A.M., Su S.Y.* Shift Registers Designed for on-line Fault Detection. Proceedings of 8th International Conference on Fault-Tolerant Computing. – 1978. – P. 173-178. **16.** *Арнольд В.И.* Динамика и статика полей Галуа. Курс лекций. – М.: Мехмат МГУ. – 2004. http://ftp.mccme.ru/

Статья представлена д.т.н., проф. И.А. Фурманом.

УДК 004.272.43

Визначення періодичної структури послідовності, що породжується багаточленом з мінімальним елементом розкладання / Гоготов В.В. // Вісник НТУ "ХПІ". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2009. – № 13. – С. 33 – 38.

Проведений аналіз впливу мінімального елемента розкладання в структурі розкладання на довжину послідовності, що генерується. Визначена періодична структура послідовності, що породжується багаточленом з мінімальним елементом розкладання. Отримана математична залежність, яка дозволяє визначати довжину формованої послідовності по вигляду розкладання. Іл.: 1. Бібліогр.: 16 назв.

Ключові слова: багаточлен з мінімальним елементом розкладання, періодична структура, довжина формованої послідовності.

UDC 004.272.43

The determination of periodic structure of sequence formed by a polynomial with the minimal element of decomposition / Gogotov V.V. // Herald of the National Techical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2009. – №. 13. – P. 33 – 38.

There was the analysis of influence of minimal element of decomposition in the structure of decomposition on the length of the generated sequence. The periodic structure of sequence, formed by a polynomial with the minimal element of decomposition, is determined. We got the mathematical relation allowing to determine the length of the formed sequence according to the decomposition. Figs: 1. Refs: 16 titles.

Key words: polynomial with the minimal element of decomposition, a periodic structure, the length of the formed sequence.

Поступила в редакцию 21.04.2009