УДК 004.421.5, 004.314.4

В.Б. УФИМЦЕВА, канд. техн. наук, ХНАГХ

О СВОЙСТВАХ СЕМЕЙСТВА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ОБОБЩЕННЫХ ЧИСЕЛ ФИБОНАЧЧИ И ИХ ПРИМЕНЕНИИ ДЛЯ ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

В статті розглядаються властивості лінійних рекурентних послідовностей узагальнених чисел Фібоначчі та їх використання для побудови генераторів псевдовипадкових чисел на прикладі генератора для формування змінної несучої частоти широтно імпульсної модуляції в системі управління перетворювачем електроенергії з метою зниження акустичного шуму і рівня електромагнітних перешкод.

Properties and using of linear recurrent of the generalized numbers and matrices of Fibonacci are considered in the article. Using of linear recurrent sequence for making pseudo-random number generators for design control system of random frequency PWM inverter is observe by way of example. It makes possible to decrease acoustic noise level and improve EMC in power converters.

Последовательности случайных чисел (СЧ) являются неотъемлемым инструментом решения многих задач – математических, технических, криптографических и т.д. Чаще всего необходимы последовательности случайных чисел, которые равномерно и равновероятно распределены на некотором отрезке.

Большинство природных процессов являются случайными, и, согласно теории математической статистики, они подчиняются различным законам распределения случайных величин. Для порождения случайных чисел, равномерно распределенных на отрезке [0..M], достаточно для некоторого случайного процесса, подчиняющегося закону равномерного распределения, ввести меру случайной величины. Подобные методы дадут очень хорошие статистические результаты, но потребуют колоссального времени для получения сколько-нибудь длинной последовательности. Поэтому более широкое распространение получили математические методы генерирования псевдослучайных числовых последовательностей (ПСЧП) [1]. Мгновенные значения таких псевдослучайных последовательностей в отличие от случайных могут быть предсказаны заранее. В то же время все оценки статистических характеристик конкретной реализации ПСЧП совпадают с оценками соответствующей ей случайной выборки.

Одной из областей применения генераторов псевдослучайных чисел (ГПСЧ) является формирование переменной несущей частоты широтно-импульсной модуляции (ШИМ) в системе управления преобразователем электроэнергии для решения задачи снижения акустического шума и уровня электромагнитных помех на несущей частоте ШИМ. Причем, для сохранения характеристик преобразовательного устройства изменение несущей частоты ШИМ должно носить случайный характер с равномерным законом распределения [2, 3].

В большинстве случаев при генерировании ПСЧП с равномерным распределением используется линейный рекуррентный метод. Наиболее распространены два линейных рекуррентных метода: линейный конгруэнтный метод и линейный рекуррентный метод получения линейной двоичной последовательности [1]. Механизм для создания линейной двоичной последовательности – линейный регистр с обратной связью – в западной технической литературе получили название Фибоначчиевых (Fibonacci Linear feedback shift register) по названию соответствующей числовой последовательности.

Развитие теории чисел Фибоначчи привело к разработке не только линейных сдвиговых регистров, но и к решению ряда задач в области теории поиска, криптографии, теории игр и др. Одним из достижений в этой области является открытие обобщенных чисел Фибоначчи [4].

Обобщенные числа Фибоначчи, называемые p-числами, являются линейной рекуррентной последовательностью (ЛРП) порядка $k = p+1$ с законом рекурсии:

$$F_p(i+p+1) = F_p(i+p) + F_p(i)\,, \qquad (1)$$

где $p \in Z \cap p \geq 0$ и $k \in Z$,

при следующих начальных условиях:

$$F_p(1) = F_p(2) = \ldots = F_p(p+1) = 1\,. \qquad (2)$$

Характеристические многочлены ЛРП p-чисел Фибоначчи имеют вид:

$$f(x) = x^{p+1} - x^p - 1\,. \qquad (3)$$

Рекуррентная формула (1) при начальных условиях (2) генерирует бесконечное число последовательностей, так как каждому p соответствует своя последовательность (в частности, при $p = 1$ генерируются классическая последовательность чисел Фибоначчи, а при $p = 0$ двоичная последовательность: 1, 2, 4, 8, …).

Для упрощения аппаратной и программной реализации ГПСЧ необходимо использовать ЛРП с минимальным количеством членов характеристического уравнения. При чем степени этих членов должны быть как можно ближе по значению [5]. Линейными рекуррентными последовательностями, удовлетворяющими этим требованиям, являются последовательности p-чисел Фибоначчи.

Однако не все рекуррентные соотношения приводят к формированию последовательностей, близких по своим свойствам к равномерным случайным. В связи с этим выдвигается ряд минимальных требований к рекуррентным последовательностям:

– равновероятность цифр внутри разрядов чисел последовательности;
– отсутствие внутри- и межразрядной корреляции.

Постановка задачи. Рассмотрим основные свойства ЛРП обобщенных чисел Фибоначчи, называемых *p*-числами, в конечном поле $GF(q^m)$. И их применение для разработки ГПСЧ на примере генератора псевдослучайных последовательностей в узлах формирования управляющих импульсов микропроцессорных систем управления автономными инверторами напряжения и тока с ШИМ с равномерным законом распределения, периодом повторяемости ($T \geq 280000$) и диапазоном изменения $\Delta\nu \in [0{,}4095]$. Генератор должен иметь простую программную и (или) аппаратную реализацию и удовлетворять требованиям к скорости вычислительного процесса (не более 450 тактов микропроцессора) и минимизации требуемой памяти.

При анализе линейных рекуррентных последовательностей p-чисел Фибоначчи были выделены последовательности p-чисел Фибоначчи максимального периода (М-последовательности) для $p = \overline{1{,}800}$.

Таблица 2.1

М-последовательности обобщенных чисел Фибоначчи над полем $GF(2^{p+1})$

Порядок чисел Фибоначчи *p*	Характеристический многочлен $f(x)$	Период ЛРП
1	x^2+x+1	3
2	x^3+x^2+1	7
3	x^4+x^3+1	15
5	x^6+x^5+1	63
6	x^7+x^6+1	127
14	$x^{15}+x^{14}+1$	32767
21	$x^{22}+x^{21}+1$	4194303
59	$x^{60}+x^{59}+1$	≈1,153e18
62	$x^{63}+x^{62}+1$	≈9,223e18
126	$x^{127}+x^{126}+1$	≈1,7e38
152	$x^{153}+x^{152}+1$	≈1,142e46
470	$x^{471}+x^{470}+1$	$2^{471}+1$
531	$x^{532}+x^{531}+1$	$2^{532}+1$

Анализ основных свойств последовательностей p-чисел Фибоначчи с максимальным периодом показал:

1. Период М-последовательностей равен $T = 2^{p+1}-1$.

2. Для заданного $f(x)$ существует $2^{p+1}-1$ различных последовательностей, которые являются $2^{p+1}-1$ различными сдвигами М-последовательности $F_p(\cdot)$ и имеют вид $F_p(\cdot), Q_pF_p(\cdot), Q_p^2F_p(\cdot), \ldots, Q_p^pF_p(\cdot)$.

3. Число единичных символов на периоде М-последовательности p-чисел Фибоначчи равно $N(F_p(i)=1)=2^p$, а нулевых – $N(F_p(i)=0)=2^p-1$, т.е. вес Хемминга $wt(F_p(0,1,\ldots,T-1))=2^p$. Вероятности появления 1 и 0 определяются выражениями:

$$p(F_p(i)=1)=\frac{2^p}{2^{p+1}-1}=\frac{1}{2}+\frac{1}{2^{p+2}-2}, \qquad (4)$$

$$p(F_p(i)=0)=\frac{2^p-1}{2^{p+1}-1}=\frac{1}{2}-\frac{1}{2^{p+2}-2}$$

и при увеличении p достигают значений сколь угодно близких к 1/2.

4. В последовательности p-чисел Фибоначчи максимальной длины серии из одного символа (единицы или нуля) встречаются 2^{p-1} раз, из двух единиц или нулей – 2^{p-2} раз и т.д. Серии из p нулей и $p+1$ единиц встречаются только по одному разу. Сравнивая выражения для оценки вероятности появления серий из l одинаковых символов для случайной последовательности с соответствующей вероятностью для М-последовательности, можно убедиться в их практической эквивалентности.

5. Свойство сдвига и сложения.

Для каждого целого $s(1 \leq s \leq 2^{p+1}-1)$ существует такое целое $r \neq s(1 \leq r < 2^{p+1}-1)$, что $\{F_p(i)\}+\{F_p(i-s)\}=\{F_p(i-r)\}$.

6. Двухуровневая автокорреляционная функция:

$$R_F(\tau)=\begin{cases}1, \tau = 0(\mathrm{mod}[2^{p+1}-1])\\ -\dfrac{1}{2^{p+1}-1}, \tau \neq 0(\mathrm{mod}[2^{p+1}-1])\end{cases}. \qquad (5)$$

7. Среди T ненулевых М-последовательностей p-чисел Фибоначчи, формируемых на основе порождающего полинома $f(x)$, имеется одна, обладающая свойством $F_p(i)=F_p(2i), i \in Z$. Из вида начальных векторов характеристических последовательностей p-чисел Фибоначчи для заданного $f(x)$ можно сделать вывод, что

$$F_p(0,1,2,\ldots,p)=\begin{cases}10^p, p=2k\\ 01^p, p=2k+1\end{cases}, \qquad (6)$$

где $k \in N$.

8. Децимацией последовательности p-чисел Фибоначчи по индексу $q(q \in N)$ называется формирование новой последовательности $G_p(i) = F_p(iq), i \in Z$. Любая М-последовательность периода $T = 2^{p+1} - 1$ может быть получена путем децимации по некоторому нечетному индексу q. При децимации последовательности $F_p(\cdot)$ по индексу $q = T - 1 = 2^{p+1}$ получена обратная последовательность $G_p(i) = F_p(i(T-1)) = F_p(-i)$ с обратным полиномом $g(x) = x^{p+1} f(x^{-1}) = x^{p+1} + x + 1$.

Для генерирования двоичной последовательности переменной несущей частоты ШИМ используем М-последовательность p-чисел Фибоначчи при $p = 21$ с рекуррентным законом $F_{21}(k) = F_{21}(k-1) + F_{21}(k-22)$ в поле $GF(2)$, характеристическим многочленом $x^{22} + x^{21} + 1$ с минимальной структурой генератора и максимальным периодом повторяемости $T = 4194303$.

Используя выбранный генератор псевдослучайных равнораспределенных бинарных М-последовательностей разработаем генератор r-разрядных псевдослучайных чисел (ГПСЧ) в диапазоне $\Delta\nu \in [0,4095]$, т. е. $r = 12$, распределенных также по равномерному закону.

Решением задачи синтеза генератора r-разрядных псевдослучайных чисел может быть параллельное включение r генераторов М-последовательностей, каждый из которых предназначен для формирования одного из разрядов чисел. Однако недостатками такого подхода является сложность устройства и невысокие статистические характеристики генерируемых последовательностей из-за наличия взаимной корреляции между М-последовательностями [5].

Наиболее часто на практике при построении r-разрядных ГПСЧ используется последовательный принцип формирования [5], заключающийся в формировании очередного значения из r символов, получаемых с помощью генератора М-последовательности.

Двоичное число U_k образуется на выходах r-разрядов регистра сдвига (РС) через каждые $s \geq r$ тактов работы. Последнее соотношение является условием статистической независимости смежных чисел в формируемой последовательности.

Величина $U_k = u_0(ks)u_0(ks+1)u_0(ks+2)\ldots u_0(ks+r-1)$, где $u_0(ks)$ – содержимое нулевого разряда РС в ks-й такт работы генератора, является периодической. При $(2^m - 1, s) = 1$ период числовой последовательности равен периоду бинарной $T = 2^m - 1$, а ее характеристики не зависят от начального состояния РС.

Для формирования псевдослучайных 12-разрядных чисел с использованием последовательности чисел Фибоначчи при $p = 21$ необходимо выбрать $s \geq r$ взаимно простое с периодом последовательности Фибоначчи $T = 4194303 = 3 \cdot 23 \cdot 89 \cdot 683$. Возьмем $s = 13$, являющееся простым числом. Отсюда, $(s, T) = 1$ и период 12-разрядных чисел равен периоду последовательности чисел Фибоначчи $T = 4194303$.

Программная реализация на ассемблере генерирует 12-разрядные числа за 120 тактов работы микропроцессора Analog Devices ADMC 300 и требует хранения 22 бит. Проведенный статистический анализ битовой последовательности формируемых чисел длиной $r \cdot T = 12 \cdot 4194303 = 50331636$ по статистическим тестам для случайных и псевдослучайных генераторов чисел американского Института стандартизации NIST [6] подтвердил случайный и равнораспределенный характер последовательности чисел на периоде повторяемости.

Использование разработанного генератора в системе управление электроприводом позволило существенно снизить уровень шума (до 27% от первоначального в зависимости от вида и состояния механизма).

Вывод. При анализе линейных рекуррентных последовательностей обобщенных чисел Фибоначчи были выделены последовательности максимального периода и рассмотрены их свойства. На примере разработанного ГПСЧ на основе последовательности Фибоначчи показана целесообразность их применения для разработки таких генераторов. Он характеризуется простотой аппаратной и программной реализации, достаточной величиной периода повторяемости, высокой скоростью генерирования чисел, хорошими статистическими характеристиками, совпадающими с характеристиками генератора двоичной последовательности. И хотя сгенерированная последовательность не удовлетворяет всем требованиям криптографических приложений, однако может иметь много других применений, в частности, в качестве начальных значений для криптографических ГПСЧ.

Список литературы: 1. *Кнут Д.* Искусство программирования, том 2. Получисленные методы. — М.: «Вильямс», 2007. – С. 832. **2.** *R. Lynn Kirlin, Sam Kwok, Stanislaw Legowski, Andrzej M. Trzynadlowski.* Power Spectra of a PWM Inverter with Randomized Pulse Position, IEEE Transactions on Power Electronics, volume 9, number 5, September 1994, pp 463-472. **3.** *C.M. Liaw, Y.M. Lin, C.H. Wu, K.I. Hwu.* Analysis, Design, and Implementation of Random Frequency PWM Inverter, IEEE Transaction on Power Electronics, volume 15, number 5, September 2000, pp 843-854. **4.** *Stakhov A. P., Massingue V., Sluchenkova A.* Introduction into Fibonacci coding and cryptography. – Kharkiv: Osnova, 1999. – 236 p. **5.** *Ярмолик В.Н., Демиденко С.Н.* Генерирование и применение псевдослучайных сигналов в системах испытания и контроля. Минск: Наука и техника, 1986. – 200 с. **6.** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto at al. – Nist Special Publication 800 – 22, 2001, 154 p.

Поступила в редколлегию 16.05.08