

Е. С. Лисицына, к.т.н., доцент

Черкасский государственный технологический университет

бульвар Шевченко, 460, г. Черкассы, 18006, Украина

aloyna@masterofcode.com

ОЦЕНКА СТАТИСТИЧЕСКИХ СВОЙСТВ (ПСЕВДО)СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ОБРАЗОВАННЫХ КОНКАТЕНАЦИЕЙ ЦИКЛОВ РЕГИСТРОВ СДВИГА С ОБРАТНЫМИ СВЯЗЯМИ

Производится оценка статистических свойств последовательностей (псевдо)случайных чисел, образованных конкатенацией циклов регистров сдвига с обратными связями.

Показано, что множество из $M=2^m$ слов интервала $(0-(M-1))$, где m – разрядность регистра и порядок генераторного многочлена, разбивается разными циклами не менее чем на два непересекающихся подмножества. Отсутствие пересечений подмножеств позволяет выполнять конкатенацию циклов (подмножеств) в произвольном порядке и получение «склеенного» из всех циклов единого сверхцикла длиной 2^m слов для любого генераторного полинома, независимо от его приводимости/неприводимости. Показано, что конкатенация сверхциклов, образованных всеми генераторными полиномами степени m , порождает (псевдо)случайную гиперцикловую последовательность чисел (слов) длиной $2^{(2^m-1)}$ слов, а изменение порядка «склеивания» циклов и сверхциклов придает стохастические свойства этой последовательности. Определен способ преобразования (псевдо)случайной последовательности в случайную длиной не менее чем $m! \cdot 2^{(2^m-1)}$ слов, статистические свойства которой весьма близки к свойствам истинно случайных последовательностей чисел, полученных из природного «белого» шума.

Ключевые слова: регистр сдвига с обратной связью, генераторный полином, цикл, конкатенация циклов.

Введение. Различают два типа генераторов (псевдо) случайных чисел. Первый из этих типов – это генераторы случайных чисел (ГСЧ), последовательность слов которых образуется квантованием по уровню выборок природных (естественных) источников «белого» шума. Эти генераторы порождают случайную последовательность слов, которая обладает следующими свойствами:

- строго равномерный закон распределения дискретной случайной величины (ошибка воспроизведения закона распределения равна нулю или очень близка к нему);
- последовательность слов не коррелирована (функция корреляции весьма близка к функции корреляции теоретического «белого» шума);
- период повторения последовательности из 2^m (где m – разрядность слова) слов бесконечен (по крайней мере, не менее 2^m !);
- порождаемая последовательность непредсказуема (по фрагменту любой длины нельзя точно предсказать последующее слово).

Недостатком таких ГСЧ является невоспроизводимость – невозможность воспроизведения последовательности при разнесе-

нии в пространстве и (или) времени процессов генерации/воспроизведения. Этот недостаток существенно ограничивает применение ГСЧ этого типа и приводит к необходимости создания дискретных логических устройств генерации (псевдо) случайных последовательностей чисел, частным примером которых являются регистры сдвига с обратными связями [1]. Эти генераторы порождают случайную последовательность слов, которая обладает следующими свойствами:

- закон распределения дискретной случайной величины может заметно отличаться от равномерного (ошибка воспроизведения закона распределения может существенно отличаться от нуля);
- последовательность слов коррелирована (функция корреляции может существенно отличаться от функции корреляции теоретического «белого» шума);
- период повторения последовательности конечен и не более 2^m слов;
- порождаемая последовательность непредсказуема (по фрагменту длиной $l \leq m$ можно точно предсказать всю последовательность);

- простота реализации и воспроизводимость последовательности.

Простота реализации и воспроизводимость обусловила широкое распространение такого рода устройств во всех областях техники телекоммуникаций, эти устройства более точно именуют генераторами псевдослучайных последовательностей, а порождаемые ими последовательности – псевдослучайными. Наличие недостатков, ограничивающих применение этого класса генераторов, породило непрерывный процесс их совершенствования, один из вариантов которого рассматривается в данной работе.

Выделение не решенных ранее частей общей проблемы. Процесс совершенствования генераторов псевдослучайных последовательностей (ПСП), в том числе и генераторов M -последовательностей, сводится к мерам, направленным на устранение их недостатков,

$$x^0 = g_m \cdot x^m + g_{m-1} \cdot x^{m-1} + g_{m-2} \cdot x^{m-2} + \dots + g_3 \cdot x^3 + g_2 \cdot x^2 + g_1 \cdot x, \quad (1),$$

где g_i – коэффициенты генераторного полинома ($g_i \in (0,1)$),

$$G(x) = g_m \cdot x^m + g_{m-1} \cdot x^{m-1} + g_{m-2} \cdot x^{m-2} + \dots + g_3 \cdot x^3 + g_2 \cdot x^2 + g_1 \cdot x + g_0 \cdot x^0. \quad (2).$$

Случайное изменение этого символа на противоположный символ дополняет нулем формируемую последовательность, улучшая тем самым статистику последовательности или, что то же самое, уменьшая ошибку воспроизведения дискретной случайной величины. Отметим, однако, что получить нулевую ошибку воспроизведения этим методом не удастся, поскольку для этого надо однократно дополнять нулем каждый цикл. Известно также, что для получения наиболее близкого к равновероятному распределения дискретной случайной величины, которую порождают генераторы на регистрах сдвига с обратными связями, используют неприводимые многочлены, что и определило их повсеместное применение во всех технических приложениях и практически полное неприятие приводимых полиномов.

Выполненные в работе [3] исследования показали возможность применения в схемах генерации (псевдо) случайных последовательностей чисел на основе регистров сдвига с обратными связями и приводимых и неприводимых полиномов, что обеспечивает возможность выполнения следующего перечня требований:

например, таких как неравномерное распределение слов в последовательности. В частности, у генераторов ПСП неравномерное распределение слов в последовательности есть следствие того, что генерируемая последовательность не содержит слова «нуль» (слова, состоящего из одних нулей). Это обусловлено тем, что нулевой вектор начальной загрузки (ВНЗ) порождает непрерывную последовательность из одних нулей, т.е. нуль цикл на графе состояний (в этот цикл, также как и в любой другой цикл, есть вход, но нет выхода). Первой (известной автору) попыткой улучшения статистических свойств последовательностей, порождаемых генераторами ПСП, выполненных на регистрах сдвига с обратными связями и, использующих неприводимый генераторный полином, является способ [2] случайного изменения на противоположный символа

- строго равномерный закон распределения дискретной случайной величины (ошибка воспроизведения закона распределения равна нулю или очень близка к нему);

- последовательность слов не коррелирована;

- период повторения последовательности слов бесконечен (по крайней мере, выходит за рамки возможности его измерения современными средствами);

- порождаемая последовательность непредсказуема;

- порождаемая последовательность воспроизводима.

Также здесь будут определены условия, обеспечивающие выполнение этих требований.

Постановка задачи. Задачей настоящего исследования является оценка статистических свойств (псевдо) случайных последовательностей чисел, порождаемых генераторами на основе регистров сдвига с обратной связью при использовании приводимых и неприводимых полиномов и конкатенации в произвольном (случайном) порядке всех циклов графа состояний.

Решение задачи. Прежде всего, отметим, что в [3] определено, что циклом ГСЧ является упорядоченное по времени подмножество слов,

порождаемых ГСЧ при неизменном значении ВНЗ, загружаемом при его пуске. Изменение ВНЗ, при фиксированном значении генераторного многочлена, позволяет выявить все циклы, порождаемые ГСЧ, и выявить, таким образом, граф состояний генератора. Важно, что множество из $M = 2^m$ генерируемых слов интервала $(0-(M-1))$, где m – разрядность регистра и разрядность генераторного многочлена, разбивается разными циклами на непересекающиеся подмножества. Разделение области определения случайной величины на непересекающиеся подмножества обеспечивает возможность выполнения конкатенации циклов и «склеивания», в произвольном порядке, отдельных циклов в единый сверхцикл длиной $T = 2^m$, независимо от приводимости или неприводимости генераторного многочлена. Выполнение конкатенации сверхциклов при переборе всех генераторных многочленов степени m (часть из них приводимые, а часть – неприводимые) позволяет получить «склеенный» гиперцикл длиной $T = 2^{(2^m-1)}$ слов. Наконец, если в каждом гиперцикле задать разный порядок следования генераторных полиномов, циклов графа каждого из этих полиномов и ВНЗ, то эти меры придают стохастический характер генерируемой последовательности и обеспе-

чивают выполнение практически всех требований, предъявляемых к современным ГСЧ. Период повторения такой гиперцикловой последовательности будет разный, для разных значений m и конструкций устройства, выполняющего перестановки генераторных полиномов, циклов графа и ВНЗ. Максимальное значение периода гиперцикловой последовательности определяется числом перестановок слов в гиперцикловой последовательности, которое равно $2^{(2^m-1)}$!. Положим, что производительность современных компьютеров не превышает 10^{11} операций в секунду, вычисление одного слова в регистровых схемах не превышает времени выполнения одной машинной операции, а год содержит всего $3,15 \cdot 10^7$ секунд. Тогда за один год компьютер может сгенерировать не более $3,15 \cdot 10^{18}$ слов/год. Допустим, что для вычислений привлечена машинная группировка из 100 компьютеров. Тогда суммарная производительность такого комплекса составит $3,15 \cdot 10^{20}$ слов/год. Для этой производительности определим период повторения гиперцикловой последовательности для разных значений m . Данные расчетов сведем в табл. 1.

Таблица 1

№	m	$2^{(2^m-1)}$	Период повторения (лет)
1	3	$2,6 \cdot 10^{35}$	$8,35 \cdot 10^{14}$
3	4	$3,85 \cdot 10^{215}$	$1,2 \cdot 10^{195}$
2	5	$3,47 \cdot 10^{1166}$	$1,1 \cdot 10^{1146}$
3	6	$1,67 \cdot 10^{5894}$	$5,3 \cdot 10^{5873}$

Как следует из этой таблицы, выполнить экспериментальную оценку периода повторения гиперцикловой последовательности практически невозможно, поскольку последовательность практически бесконечна и ее свойства практически совпадают со свойствами последовательностей, образованных квантованием природных (естественных) источников «белого» шума, воспроизводимость последовательности определяется воспроизводимостью порядка следования перестановок. В тех случаях, когда можно допустить уменьшение периода повторения гиперцикловой последовательности на несколько порядков, выполнение процедур тасовки (перемешивания) генераторных полиномов, циклов графа и ВНЗ существенно упрощается и может быть выполнено с помощью методов,

изложенных в [4], в этом случае воспроизводимость процесса гарантирована.

Для проверки основных положений этой концепции выполнена программная модель ГСЧ, упрощенная схема которой приведена на рис. 1. В этой модели перемешивание генераторных полиномов, циклов графа и ВНЗ осуществлялось в конце каждого гиперцикла с помощью компьютерной программы генерации случайных чисел *random*, что не отражено на рисунке. При этом задача обеспечения воспроизводимости не ставилась и порядок выполнения перестановок не определялся.

Все данные, необходимые для реализации ГСЧ для $m = 5$ приведены в приложении А, заимствованном в [5].

Основными узлами ГСЧ для $m = 5$ являются 5-разрядный регистр сдвига РС, с

включенным в цепь обратной связи набором ключей Кл и сумматором по модулю 2, постоянное запоминающее устройство ПЗУ1, ПЗУ2

и схема управления, состоящая из трех двоичных счетчиков Сч1, Сч2, Сч3 и двух схем сравнения Ср1 и Ср2.

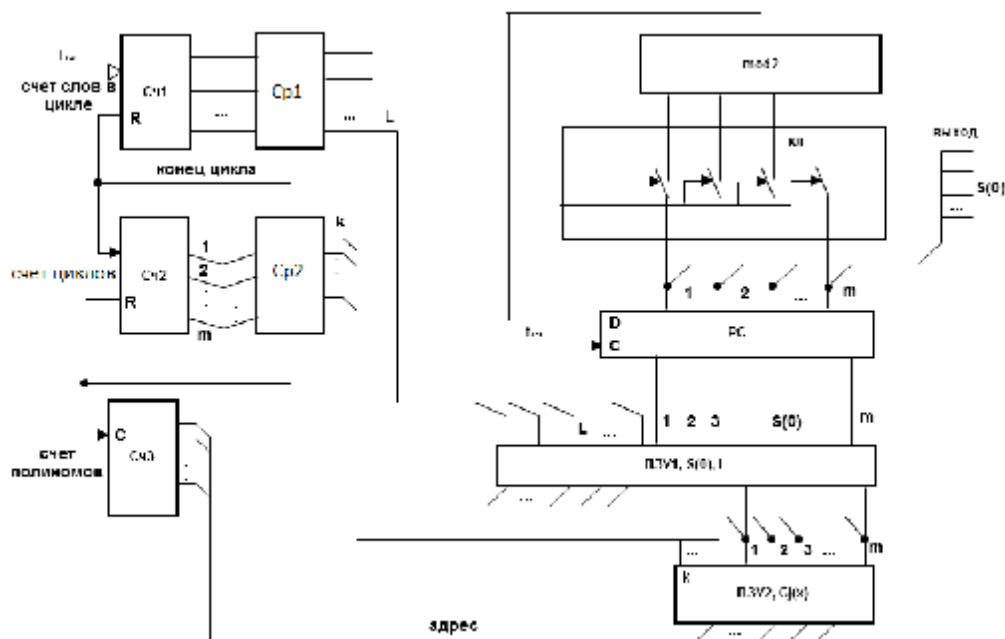


Рис. 1. Упрощенная схема ГСЧ

В момент запуска генератора счетчики Сч1, Сч2, Сч3 устанавливаются в нулевое состояние, а в ПЗУ1 и ПЗУ2 заносятся управляющие процессом генерации данные (для $m = 5$ эти данные приведены в приложении А). Так, в ПЗУ2 заносится перечень полиномов и данные о числе циклов, порождаемых каждым из них. В ПЗУ1 заносятся ВНЗ каждого цикла и его длина. В момент начала работы из ПЗУ2 извлекается первый генераторный полином $G(x) = x^5 + 1$ (код 10001) и указатель общего числа циклов, порождаемых этим многочленом (здесь $k = 8$). Для первого генераторного многочлена замыкаются 1 и 5-й ключи, в результате чего образуется регистр сдвига с обратной связью с генераторным многочленом $G(x) = x^5 + 1$. Для данного генераторного многочлена из ПЗУ1 извлекается первый ВНЗ и указатель длины (здесь первым идет нуль цикл длиной $L = 1$ и $S(0) = 0$). Первым тактом слово $S(0) = 0$ выводится на выход ГСЧ, счетчик Сч1 получает приращение +1, срабатывает схема сравнения Ср1, возвращая в нулевое состояние Сч1 и добавляя +1 к состоянию Сч2. Изменение состояния Сч2 приводит к смене адреса ячейки ПЗУ1, из которой извлекается представитель следующего цикла и указатель его длины (здесь следующий цикл

имеет длину $L = 5$ и $S(0) = 1$). Поступающими тактами сдвига выполняется вычисление и вывод на выход ГСЧ следующих пяти слов (1 2 4 8 16) до тех пор, пока в Сч1 не накопится число 5, после чего схема сравнения Ср1 сформирует сигнал «конец цикла» и изменит адрес ПЗУ1.

В результате извлекается новое значение представителя следующего цикла и указатель его длины (здесь следующий цикл имеет длину $L = 5$ и $S(0) = 3$). Так продолжается до тех пор, пока не будет сгенерирован последний – восьмой цикл этого генераторного многочлена (это нуль цикл, порожденный $S(0) = 31$). В момент его окончания срабатывает схема сравнения Ср2, счетчики Сч1 и Сч2 возвращаются в нулевое состояние, а счетчик Сч3 получает приращение +1. В результате этого из ПЗУ1 извлекается следующий полином (это $G(x) = x^5 + x + 1$), далее процесс повторяется до тех пор, пока не будет сгенерирован гиперцикл из 2^9 слов. По окончании формирования гиперцикла производится перемешивание генераторных полиномов, циклов графа и ВНЗ (это перестановка строк в ПЗУ1 и замена слов $S(0)$ в ПЗУ2). Для примера здесь показана одна строка, сформированная компьютерной программой random из 16 слов (здесь 16 – общее число многочленов 5-й степени):

13, 7, 11, 2, 8, 12, 15, 3, 10, 0, 14, 9, 4, 6, 1, 5, из чего следует, что в ПЗУ2 в ячейку по адресу 0 перемещается слово из 13-й ячейки (вместо $G(x) = x^5 + 1$ записывается 13-й полином $G(x) = x^5 + x^4 + x^3 + x + 1$). Этот многочлен неприводим и поэтому здесь $k = 2$ и тасовка сводится к перестановке местами нуль цикла и цикла с $L = 31$. Компьютерной программой random формируется одно случайное число $S(0) \leq 31$, которое используется при генерации первого сверхцикла. Эти меры позволяют обеспечить случайный перебор слов в гиперцикловой последовательности и придание, таким образом, тех же статистических свойств последовательности, как и в последовательности, образованной квантованием по уровню выборок природных (естественных) источников «белого» шума, за исключением распределения k -грамм. Здесь, под k -граммой будем подразумевать группу из k любых, наперед заданных, слов из области определения генерируемой случайной величины. Для истинно случайных процессов распределение k -грамм подчиняется закону

$$p(k) = M^{-k} \quad (3)$$

Последовательность слов, порождаемая генератором, выполненным по схеме, приведенной на рис. 1, отличается от истинно случайной последовательности тем, что каждый сверхцикл есть последовательность из $M = 2^m$ генерируемых слов интервала $(0, (M-1))$, в котором каждое из слов повторяется строго по одному разу. Это обусловлено тем, что циклы регистра сдвига с обратными связями разбивают область определения функции на непересекающиеся подмножества, следствием этого также является то, что закон распределения дискретной случайной величины строго равномерный (ошибка воспроизведения закона распределения равна нулю). В силу этого обстоятельства появление k -грамм вида «a...a...a» при $k > 2$ невозможно ($p_{aa}(k > 2) = 0$), а распределение k -грамм вида «a...v...c» определяется как

$$p_{abc}(k \geq 2) = \prod_{i=0}^{k-1} (M - i)^{-1} \quad (4)$$

Таким образом, регистр сдвига с обратными связями, выполненный в соответствии с изложенной концепцией, строго говоря, генерирует псевдослучайную последовательность. Если учесть, что перестановки генераторных полиномов, циклов графа и

ВНЗ существенно разрушают корреляцию слов сверхцикловой и гиперцикловой последовательностей, то можно найти такой интервал τ между словами, при котором степень корреляции слов ничтожно мала и, поэтому, последовательности, смещенные друг относительно друга на интервал τ слов, статистически независимы. Тогда композиция двух последовательностей вида

$$S(x) = |A_0(x) + A_\tau(x)|_M \quad (5)$$

преобразует псевдослучайные последовательности $A_0(x), A_\tau(x)$ в случайную последовательность $S(x)$, для которой распределение k -грамм определяется выражением (3). Эта последовательность удовлетворяет всем требованиям, предъявляемым в данной работе к случайным последовательностям.

Полученные результаты. Проведенные исследования показали возможность построения генераторов случайных чисел на основе регистров сдвига с обратными связями иconcatenацией циклов всех генераторных многочленов степени m и обеспечили возможность создания нового способа формирования последовательности случайных чисел [6].

Эти генераторы обеспечивают два режима работы:

- режим генерации ПСП;
- режим генерации случайной последовательности.

В режиме генерации ПСП генерируемая последовательность соответствует всем свойствам случайных последовательностей, за исключением распределения k -грамм.

В режиме ПСП вероятность появления k -грамм вида «a...a...a» равна нулю, а распределение k -грамм вида «a...v...c» соответствует выражению (4). В режиме генерации случайной последовательности дополнительно выполняется процедура вычисления композиции, определенной выражением (5), что обеспечивает распределение k -грамм в соответствии с выражением (3). Оптимальное значение задержки τ , обеспечивающее минимум ошибки воспроизведения закона распределения дискретной случайной величины, не является постоянной величиной, для разных m эту задержку приходилось определять экспериментально, что свидетельствует о неполном подавлении корреляции между словами последовательности. Ошибка воспроизведения закона распределения дискретной величины ϵ вычислялась в соответ-

ствии с работой [7], как приходящееся на единицу объема выборки среднее число ошибочных слов, трансформирующих гипотетическое распределение дискретной случайной величины в эмпирическое.

Период повторения гиперцикловой последовательности и в режиме ПСП, и в режиме генерации случайной последовательности соответствует данным табл. 1, с оговоркой, что получить экспериментальное подтверждение этого факта в данной работе не представлялось возможным.

Нулевая ошибка воспроизведения дискретной случайной величины в режиме генерации ПСП была гарантирована алгоритмом работы генератора и, поэтому, не требовала экспериментального подтверждения.

Статистические свойства случайной последовательности (в режиме генерации случайной последовательности) определялись экспериментально, при объеме выборки, равном $5000 \cdot 2^{(2m-1)}$ слов, и оптимальном значении величины задержки для каждого значения m . Результаты испытаний приведены в табл. 2.

Таблица 2

m	3	4	5	6	7
τ	19	25	42	118	216
ε	0,0055 (55 ошибок на 10 000 слов)	0,0011 (11 ошибок на 10 000 слов)	0,00085 (85 ошибок на 100 000 слов)	0,00065 (65 ошибок на 100 000 слов)	0,0006 (6 ошибок на 10 000 слов)

Выводы. Выполненное исследование показало:

1. Применение в ГСЧ, выполненных на регистрах сдвига с обратными связями, конкатенации циклов, перестановки генераторных полиномов, циклов графа и ВНЗ обеспечивают возможность построения генераторов случайных чисел с двумя режимами работы – генерация псевдослучайной и генерация случайной последовательности чисел.

2. В режиме генерации ПСП выполняются все требования к случайным последова-

тельствам, сформулированные в данной работе, кроме распределения k -грамм.

3. В режиме генерации случайной последовательности выполняются все требования к случайным последовательностям, сформулированные в данной работе, кроме требования по обеспечению нулевой ошибки распределения дискретной случайной величины. При этом ошибка воспроизведения уменьшается с ростом степени генераторного полинома.

Приложение А

Порядок полинома: $m = 5$.

$G(x) = x^5 + 1$. $A(n): [0][1\ 2\ 4\ 8\ 16][3\ 6\ 12\ 24\ 17][5\ 10\ 20\ 9\ 18][7\ 14\ 28\ 25\ 19][11\ 22\ 13\ 26\ 21][15\ 30\ 29\ 27\ 23][31]$.

$\Gamma = 6x^5 + 2x^1$

$G(x) = x^5 + x + 1$. $A(n): [0][1\ 3\ 7\ 15\ 31\ 30\ 29\ 26\ 21\ 10\ 20\ 9\ 19\ 6\ 12\ 24\ 17\ 2\ 4\ 8\ 16][5\ 11\ 23\ 14\ 28\ 25\ 18][13\ 27\ 22]$.

$\Gamma = 1x^{21} + 1x^7 + 1x^3 + 1x^1$

$G(x) = x^5 + x^2 + 1$. $A(n): [0][1\ 2\ 5\ 10\ 21\ 11\ 23\ 14\ 29\ 27\ 22\ 12\ 24\ 17\ 3\ 7\ 15\ 31\ 30\ 28\ 25\ 19\ 6\ 13\ 26\ 20\ 9\ 18\ 4\ 8\ 16]$.

$\Gamma = 1x^{31} + 1x^1$

$G(x) = x^5 + x^2 + x + 1$. $A(n): [0][1\ 3\ 6\ 13\ 27\ 23\ 15\ 30\ 28\ 25\ 18\ 4\ 8\ 16][2\ 5\ 11\ 22\ 12\ 24\ 17][7\ 14\ 29\ 26\ 20\ 9\ 19][10\ 21][31]$.

$\Gamma = 1x^{14} + 2x^7 + 1x^2 + 2x^1$

$G(x) = x^5 + x^3 + 1$. $A(n): [0][1\ 2\ 4\ 9\ 18\ 5\ 11\ 22\ 12\ 25\ 19\ 7\ 15\ 31\ 30\ 28\ 24\ 17\ 3\ 6\ 13\ 27\ 23\ 14\ 29\ 26\ 21\ 10\ 20\ 8\ 16]$.

$\Gamma = 1x^{31} + 1x^1$

$G(x) = x^5 + x^3 + x + 1$. $A(n): [0][1\ 3\ 7\ 14\ 29\ 27\ 22\ 12\ 25\ 18\ 5\ 10\ 20\ 8\ 16][2\ 4\ 9\ 19\ 6\ 13\ 26\ 21\ 11\ 23\ 15\ 30\ 28\ 24\ 17][31]$.

$\Gamma = 2x^{15} + 2x^1$

$G(x) = x^5 + x^3 + x^2 + 1$. $A(n): [0][1\ 2\ 5\ 11\ 23\ 15\ 30\ 29\ 26\ 20\ 8\ 16][3\ 7\ 14\ 28\ 24\ 17][4\ 9\ 18][6\ 12\ 25\ 19][10\ 21][13\ 27\ 22][31]$.

$\Gamma = 1x12 + 1x6 + 1x4 + 2x3 + 1x2 + 2x1$

$G(x) = x^5 + x^3 + x^2 + x + 1$. $A(n): [0][1\ 3\ 6\ 12\ 25\ 18\ 4\ 9\ 19\ 7\ 15\ 31\ 30\ 29\ 27\ 23\ 14\ 28\ 24\ 17\ 2\ 5\ 10\ 21\ 11\ 22\ 13\ 26\ 20\ 8\ 16]$.

$\Gamma = 1x31 + 1x1$

$G(x) = x^5 + x^4 + 1$. $A(n): [0][1\ 2\ 4\ 8\ 17\ 3\ 6\ 12\ 25\ 18\ 5\ 10\ 21\ 11\ 23\ 15\ 31\ 30\ 28\ 24\ 16][7\ 14\ 29\ 26\ 20\ 9\ 19][13\ 27\ 22]$.

$\Gamma = 1x21 + 1x7 + 1x3 + 1x1$

$G(x) = x^5 + x^4 + x + 1$. $A(n): [0][1\ 3\ 7\ 15\ 30\ 28\ 24\ 16][2\ 4\ 8\ 17][5\ 11\ 22\ 13\ 26\ 20\ 9\ 18][6\ 12\ 25\ 19][10\ 21][14\ 29\ 27\ 23][31]$.

$\Gamma = 2x8 + 3x4 + 1x2 + 2x1$

$G(x) = x^5 + x^4 + x^2 + 1$. $A(n): [0][1\ 2\ 5\ 10\ 20\ 9\ 19\ 6\ 13\ 27\ 23\ 14\ 28\ 24\ 16][3\ 7\ 15\ 30\ 29\ 26\ 21\ 11\ 22\ 12\ 25\ 18\ 4\ 8\ 17][31]$.

$\Gamma = 2x15 + 2x1$

$G(x) = x^5 + x^4 + x^2 + x + 1$. $A(n): [0][1\ 3\ 6\ 13\ 26\ 21\ 10\ 20\ 9\ 18\ 4\ 8\ 17\ 2\ 5\ 11\ 23\ 15\ 31\ 30\ 29\ 27\ 22\ 12\ 25\ 19\ 7\ 14\ 28\ 24\ 16]$.

$\Gamma = 1x31 + 1x1$

$G(x) = x^5 + x^4 + x^3 + 1$. $A(n): [0][1\ 2\ 4\ 9\ 19\ 7\ 15\ 30\ 29\ 27\ 22\ 12\ 24\ 16][3\ 6\ 13\ 26\ 20\ 8\ 17][5\ 11\ 23\ 14\ 28\ 25\ 18][10\ 21][31]$.

$\Gamma = 1x14 + 2x7 + 1x2 + 2x1$

$G(x) = x^5 + x^4 + x^3 + x + 1$. $A(n): [0][1\ 3\ 7\ 14\ 28\ 25\ 19\ 6\ 13\ 27\ 23\ 15\ 31\ 30\ 29\ 26\ 20\ 8\ 17\ 2\ 4\ 9\ 18\ 5\ 10\ 21\ 11\ 22\ 12\ 24\ 16]$.

$\Gamma = 1x31 + 1x1$

$G(x) = x^5 + x^4 + x^3 + x^2 + 1$. $A(n): [0][1\ 2\ 5\ 11\ 22\ 13\ 26\ 21\ 10\ 20\ 8\ 17\ 3\ 7\ 14\ 29\ 27\ 23\ 15\ 31\ 30\ 28\ 25\ 18\ 4\ 9\ 19\ 6\ 12\ 24\ 16]$.

$\Gamma = 1x31 + 1x1$

$G(x) = x^5 + x^4 + x^3 + x^2 + x + 1$. $A(n): [0][1\ 3\ 6\ 12\ 24\ 16][2\ 5\ 10\ 20\ 8\ 17][4\ 9\ 18][7\ 15\ 30\ 28\ 25\ 19][11\ 23\ 14\ 29\ 26\ 21][13\ 27\ 22][31]$.

$\Gamma = 4x6 + 2x3 + 2x1$

Список литературы

1. Лидл Р. Конечные поля : в 2 т. / Р. Лидл, Г. Нидеррайтер ; [пер. с англ. под ред. Нечаева В. И.] – М. : Мир, 1988. – 822 с.
2. Пат. 36108 Україна, МПК G06F 7/58 (2006.01), G07C 15/00. Спосіб генерації випадкових чисел та пристрій для його здійснення / Торба О. О. ; заявник та патентовласник Харківський державний технічний університет радіоелектроніки. – № 99116006 ; заявл. 02.11.1999 ; опубл. 16.04.2001, Бюл. № 3.
3. Лисицына Е. С. Исследование циклов генераторов на регистрах сдвига с обратными связями / Е. С. Лисицына // Вісник Хмельницького національного університету. – 2014. – №1. – С. 121-125.
4. Лисицына Е. С. Генерация перестановок в стохастических генераторах / Е. С. Лисицына // Вісник Черкаського державного технологічного університету. – 2013. – № 2. – С. 10–13.
5. <https://dl.dropboxusercontent.com/u/11291120/rezults.rar>
6. Пат. 86705 Україна, МПК G06F 7/58 (2006.01). Спосіб формування послідовності випадкових чисел / Лега Ю. Г., Швидкий В. В., Фауре Е. В., Лісіцина О. С., Лавданський А. О. ; заявник та патентовласник ЧДТУ. – № u201307989 ; заявл. 25.06.2013 ; опубл. 10.01.2014, Бюл. № 1.
7. Фауре Э. В. Оценка точности воспроизведения закона распределения дискретной случайной величины при ее преобразовании / Э. В. Фауре, А. С. Береза, Е. А. Ярославская // Вісник Хмельницького національного університету. – 2012. – № 5. – С. 176–182.

References

1. Lidl, R. and Niederreiter, H. (1988), Finite fields. Moscow: Mir, 822 p. [in Russian].
2. Torba, O. O. (2001) A method for generating random numbers and a device for its realiza-

- tion. Patent of Ukraine No. 36108, Bull. No. 3 from 16.04.2001 [in Ukrainian].
3. Lisitsyna, O. (2013) The study of the cycles of generators with feedback shift registers. *Visnyk Khmelnyts'koho natsional'noho universitetu*, (1), pp. 121-125 [in Russian].
 4. Lisitsyna, O. (2013) Permutations generated in stochastic oscillators. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, (2) [in Russian].
 5. <<https://dl.dropboxusercontent.com/u/11291120/rezults.rar>>
 6. Lega, Yu. G., Shvydkyi, V. V., Faure, E. V. et al. (2014) A method for forming random numbers sequence. Patent of Ukraine No. 86705, Bull. No. 1 from 10.01.2014 [in Ukrainian].
 7. Faure, E., Bereza, A. and Yaroslavskaya, E. (2012) Evaluation of the fidelity of reproduction of the law of distribution of discrete random variable at its transformation. *Visnyk Khmelnyts'koho natsional'noho universitetu*, (5), pp. 176-182 [in Russian].

Стаття надійшла до редакції 18.04.2014.

E. S. Lisitsyna, Ph.D., associate professor
Cherkasy State Technological University
Schevchenko blvd, 460, Cherkasy, 18006, Ukraine
aloyna@masterofcode.com

EVALUATION OF STATISTICAL PROPERTIES OF (PSEUDO) RANDOM SEQUENCES FORMED BY THE CONCATENATION OF THE CYCLES OF FEEDBACK SHIFT REGISTERS

The solution of many practical problems is impossible without using of random number sequences. Most often, to solve the applied problems people use uniformly distributed random numbers sequence, which can be generated by a feedback shift register.

If generator polynomial is irreducible, then such generator produces a sequence number equal to the maximum length $T=(2^m-1)$, where m – the order of polynomial generator. If this generator is set to the initial state $S(0)=0$, then it will continuously generate a sequence consisting of zeros. This allows to present state graph of the generator in the form of two loops, one of which has a length $T=(2^m-1)$, and the other consists of one null character. State graph of the generator can be represented as: $\Gamma=1 \times (2^m-1) + 1 \times 1$. If generator polynomial is integral, then state graph may consist of several cycles. It is important that regardless of the reducibility or irreducibility of generator polynomial, these cycles divide sequence of 2^m words into disjoint subsequences. This allows us to produce a concatenation of all cycles of the graph in a supercycle, the length of which is equal to 2^m . Using all generating polynomials of degree m , and concatenating all supercycles in a single hypercycle, we are able to construct a sequence of length $T=2^{(2^m-1)}$ words. If each hypercycle would be reordered by the concatenations of supercycles and initial state, we can get a sequence having stochastic properties and having a length of up to $T=(2^{(2^m-1)})!$ words. These approaches allow to create a new method for generating a sequence of random numbers, patented in Ukraine.

In the article the results of practical evaluation of statistical properties of a random sequence of numbers are obtained as a result of the implementation of this method. In particular, it is shown that the law of distributing of random sequence is almost equal to theoretical distributing, and the repetition period of the sequence at $m \geq 5$ is millions of years at the maximum speed of shift register.

Keywords: feedback shift register, generator polynomial, cycle, cycles concatenation.