УДК 621.391:004.73

Е.С. ЛИСИЦЫНА
Черкасский государственный технологический университет

ИССЛЕДОВАНИЕ ЦИКЛОВ ГЕНЕРАТОРОВ НА РЕГИСТРАХ СДВИГА С ОБРАТНЫМИ СВЯЗЯМИ

Исследуются циклы, порождаемые регистром сдвига с обратными связями для всего множества генераторных полиномов степени m. Показано, что множество из M=2^m слов интервала (0-(M-1)), разбивается разными циклами не менее чем на 2 непересекающихся подмножества. Отсутствие пересечений подмножеств, создает предпосылки для конкатенации циклов (подмножеств) и получения «склеенного» из всех циклов единого сверхцикла длиной 2^m слов для любого генераторного полинома, независимо от его приводимости/неприводимости.

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

OLENA LISITSYNA
Cherkasy State Technological University

THE RESEARCH OF THE CYCLES GENERATED VY FEEDBACK SHIFT REGISTERS

Abstract – I investigate the cycles generated by a feedback shift register for the whole set of generator polynomials of degree m. The research results:

1. Using of the concatenation of cycles with random numbers generator by a feedback shift register, regardless of reducibility/irreducibility of the generator polynomial of degree m allows us to get "cemented" cycle (super cycle) 2m words long.

2. Using of the concatenation of super cycles generated by generator polynomials of the same degree m, allows us to "glue" and get super cycles T=2^{2m-1} long words.

3. In all of these cases random numbers generator by feedback shift register generates a sequence of numbers distributed uniformly within the interval of (0 - (M-1)) with zero error of reproducing the discrete random variable; the sequence is reproducible and predictable, and its correlation is significantly less than all known random numbers generator of this class, while a sequence repetition period is significantly bigger.

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

Введение

Генераторы псевдослучайных последовательностей (ПСП), выполненные на регистрах сдвига с обратными связями, используются во всех системах телекоммуникаций, принципы их построения и свойства хорошо известны [1]. ПСП, порожденные неприводимым генераторным полиномом, имеют близкое к равномерному распределение дискретной случайной величины на интервале $\overline{(0,(M-1))}$, причем степень близости растет с ростом степени генераторного полинома. Кроме того эти последовательности имеют «хорошую» автокорреляционную функцию (АКФ), такую, что уровень боковых лепестков $\rho(\tau>0)=\left|\frac{1}{M}\right|$, при этом качество АКФ (соотношение уровня основного лепестка и боковых) так же улучшается с ростом степени полинома. Эти свойства в сочетании с простотой построения генераторов на регистрах сдвига привели к их повсеместному применению в системах связи различного назначения.

Выделение не решенных ранее частей общей проблемы

Несмотря на то, что к настоящему времени накоплен большой арсенал технических решений, обеспечивающих создание средств генерации случайных последовательностей чисел (ГСЧ), основанных на использовании регистров сдвига с обратными связями многие теоретические вопросы остаются нерешенными. В частности, не решены вопросы обеспечения следующего ряда требований к ГСЧ:

- распределение дискретной случайной величины на интервале $\overline{(0,(M-1))}$ должно быть равномерным, а ошибка воспроизведения должна быть равна нулю;
- последовательность случайных чисел должна быть некоррелированной;
- последовательность должна быть воспроизводимой;
- последовательность должна быть непредсказуемой;
- период повторения последовательности должен быть бесконечным.

Сразу отметим, что здесь приведен, скорее всего, перечень недостижимых свойств дискретного случайного процесса, но это хороший стимул поиска технических решений, обеспечивающих улучшение характеристик формирователей случайных последовательностей чисел. Заметим, что наиболее близка, по своим свойствам, к сформулированным здесь требованиям последовательность случайных чисел, полученная квантованием значения энергии потока фотонов, испускаемых солнцем или лампой накаливания (при питании ее постоянным током). Эта последовательность обладает всеми нужными свойствами, за исключением свойства воспроизводимости. Эта последовательность невоспроизводима, т.е. нельзя точно воспроизвести ни один фрагмент последовательности при разнесении событий производства/воспроизводства в пространстве и времени. Отсюда следует, что такие последовательности случайных чисел не могут быть использованы для моделирования дестабилизирующих факторов, в ходе многократных испытаний сложных систем и устройств или для создания систем криптографической зашиты информации. Генераторы случайных последовательностей чисел, выполненные на дискретной логике, в том числе генераторы на регистрах сдвига с обратными связями, воспроизводимы, предсказуемы (способ образования последовательности вычислим по любому ее отрезку не более чем из m слов), ошибка воспроизведения закона распределения дискретной случайной величины отлична от нуля, последовательность слов конечна и коррелирована.

Целью настоящей работы является исследование путей получения последовательности случайных чисел с помощью генератора на регистрах сдвига с обратными связями с нулевой ошибкой распределения дискретной случайной величины на интервале $\overline{(0,(M-1))}$, уменьшение корреляции слов последовательности и, как следствие, ее предсказуемости, увеличение периода повторения последовательности до значений, существенно превышающих величину M .

Постановка задачи

Задачей исследования является определение графа состояний генератора на регистре сдвига с обратной связью, как совокупности разрозненных циклов, определение возможности конкатенации циклов, определение свойств получаемой последовательности, для любого генераторного полинома степени m и при большом числе генераторных полиномов.

Решение задачи

Прежде всего, отметим, что в [3] определено, что циклом ГСЧ является упорядоченное по времени подмножество порождаемых генератором слов из множества мощности *M*. Пусть ГСЧ выполнен в виде регистра сдвига с обратной связью, пусть его генераторный полином

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

Как следует из [2], регистр сдвига с обратными связями есть устройство, решающее характеристическое уравнение вида:

$$x^0 = g_m \cdot x^m + g_{m-1} \cdot x^{m-1} + g_{m-2} \cdot x^{m-2} + \cdots + g_3 \cdot x^3 + g_2 \cdot x^2 + g_1 \cdot x \qquad (2).$$

Это значит, что у регистра сдвига с обратными связями и генераторным полиномом степени m всегда $g_m = g_0 = 1$, и

$$G(x) = x^m + g_{m-1} \cdot x^{m-1} + g_{m-2} \cdot x^{m-2} + \cdots + g_3 \cdot x^3 + g_2 \cdot x^2 + g_1 \cdot x + 1 \qquad (3).$$

Представим генераторный полином в виде: $G(x) = (x^m + 1) + A(x)$, где: $A(x) = g_{m-1} \cdot x^{m-1} + g_{m-2} \cdot x^{m-2} + \cdots + g_3 \cdot x^3 + g_2 \cdot x^2 + g_1 \cdot x = x \cdot A_0(x)$, тогда:

$$G(x) = x^m + x \cdot A_0(x) + 1 \qquad (4).$$

Полином $A_0(x)$, входящий в равенство (4), может быть представлен в форме десятичного числа:

$$A_0 = g_{m-1} \cdot 2^{m-2} + g_{m-2} \cdot 2^{m-3} + \cdots + g_3 \cdot 2^2 + g_2 \cdot 2 + g_1 \qquad (5).$$

которое при изменении генераторного полинома пробегает все значения интервала $\overline{0,(2^{(m-1)}-1)}$, в связи с чем общее число генераторных полиномов вида (4) равно: $r = 2^{(m-1)}$ (6).

С учетом изложенного, здесь будут исследоваться циклы, порождаемые генераторным полиномом вида (4) при решении характеристического уравнения (2) для $A_0 \in \overline{0,(2^{(m-1)}-1)}$.

Отметим, также, что регистр сдвига с обратными связями обеспечивает два способа съема случайной последовательности:

- в виде последовательности случайных двоичных символов «нуля» и «единицы»;
- в виде последовательности случайных чисел, которые могут быть представлены в полиномиальной или десятичной форме.

Последовательность двоичных символов «нуля» и «единицы» снимается с любого отвода регистра сдвига и последовательности, снятые с разных отводов отличаются только циклическим сдвигом.

Последовательность случайных чисел может быть получена, если в каждый дискретный момент времени n, прочитать в отводах регистра (первого, второго .. m-го отвода) кодовую комбинацию двоичных символов которую, затем представить в полиномиальной или десятичной формах. В полиномиальной форме для кодовой комбинации нулей и единиц $s_m, s_{m-1}, s_{m-2}, s_{m-3}, \cdots s_3, s_2, s_1$ получим полином вида $S_n^{\wedge}(x) = s_m \cdot x^m + s_{m-1} \cdot x^{m-1} + s_{m-2} \cdot x^{m-2} + \cdots + s_3 \cdot x^3 + s_2 \cdot x^2 + s_1 \cdot x^1 = x \cdot S_n(x)$, где: $S_n(x) = s_m \cdot x^{m-1} + s_{m-1} \cdot x^{m-2} + s_{m-2} \cdot x^{m-3} + \cdots + s_3 \cdot x^2 + s_2 \cdot x + s_1 \cdot x^0$. Для десятичной формы представления полинома $S_n(x)$ получим

$$A(n) = s_m \cdot 2^{m-1} + s_{m-1} \cdot 2^{m-2} + s_{m-2} \cdot 2^{m-3} + \cdots + s_3 \cdot 2^2 + s_2 \cdot 2^1 + s_1 \cdot 2^0 \qquad (7).$$

Именно в этой форме будем записывать здесь результаты расчета случайной последовательности чисел.

Отметим, что ГСЧ, выполненный на регистре сдвига с обратными связями, вычисляет последующее слово по предыдущему, т.е. реализует операцию $S(n) = f[S(n-1)]$ (8) , что и определяет предсказуемость его поведения. Вычисление последующего слова по предыдущему сводится к выполнению следующих операций:

- решая уравнение (2), вычисляется двоичный символ s_0;
- вычисляется $S(n) = \left|x \cdot S(n-1)\right|_{x^m+1}$ (9), далее процесс повторяется.

Выражение (9) говорит о том, что сначала выполняется сдвиг на один шаг (в сторону старших разрядов) слова $S(n-1)$, а затем из полученного результата выделяется слово из младших (m-1) символов.

Заметим, что для вычисления первого сгенерированного слова $S(1)$, в регистр сдвига с обратной связью вносится извне слово $S(0)$, которое называют вектор начальной загрузки (ВНЗ) и, выбор которого определяет внешний субъект по своему усмотрению. Как следует из уравнения (2) выбор ВНЗ $S(0)=0$ порождает нуль цикл, цикл, состоящий из одного слова $S=0$. Отсюда следует вывод, что все генераторы на регистрах сдвига с обратными связями *не зависимо от генераторного полинома* имеют нуль цикл в точке 0. Если полином неприводим, то порождаемая регистром последовательность имеет период повторения T слов, где $T=2^m-1$, которую называют М-последовательностью. Таким образом, граф состояний регистра сдвига с обратными связями и неприводимым генераторным полиномом имеет два цикла:

- цикл из T слов, порождаемый при $S(0)\neq 0$;
- цикл из одного слова $S=0$, порождаемый при $S(0)=0$.

Таким образом, регистр сдвига с обратными связями и неприводимым генераторным полиномом может генерировать равномерно распределенную последовательность чисел в интервале $\overline{(0,(M-1))}$, где $M=2^m$. Для этого достаточно выполнить конкатенацию - «склеивание» порождаемых им циклов, т.е. вставить один раз за цикл слово $S=0$. Граф состояний такого дискретного автомата будем представлять в виде Г=1x(M-1)+1x1. Эта запись обозначает, что граф дискретного автомата содержит один цикл длиной (M-1) и один цикл длиной «1». Порождаемую им последовательность будем представлять в виде $A(n):[A(0),A(1),A(2),\cdots A(M-1)],[0]$, циклы которой выделены квадратными скобками. Для определения графа состояний дискретного автомата- регистра сдвига с обратными связями для генераторных полиномов вида (4) была создана программная модель устройства для генерации циклов, упрощенная функциональная схема которого приведена на рис.1.

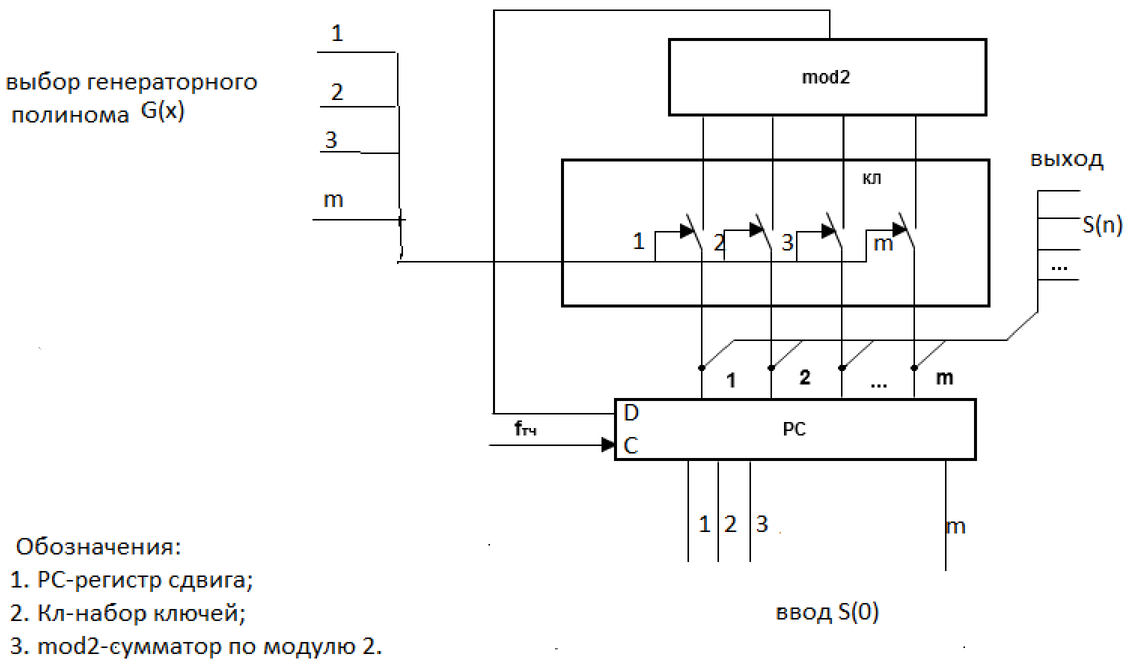

Рис. 1. Устройство для генерации циклов

Устройство для генерации циклов представляет m-разрядный регистр сдвига, каждый выход которого через ключ Кл подключен ко входу сумматора по модулю 2, выход которого подключен ко входу D регистра сдвига. Сумматор по модулю 2 производит вычисление двоичного символа S_0 по уравнению (2). При поступлении тактового импульса на вход C регистра, производится сдвиг в сторону старших разрядов и формирование слова *S(n)* в соответствии с выражением (9). В начале цикла создают управляющую ключами Кл кодовую комбинацию, определяющую генераторный полином и кодовую комбинацию, соответствующую ВНЗ *S(0)*. Наблюдая выходную последовательность *S(n)*, и, подсчитывая число слов в цикле, определяют длину этого цикла. Поскольку циклы разделяют множество из 2^m слов на непересекающиеся подмножества, то для нахождения следующего цикла в качестве ВНЗ загружают любое слово, не вошедшее в первый цикл. Для третьего цикла (если он имеется) в качестве ВНЗ загружают любое слово, не вошедшее в первые два цикла. Перебор ВНЗ продолжается до тех пор, пока не будет определена принадлежность каждого слова множества (0…(M-1)) порождаемым циклам. После выявления всех циклов записывается граф состояний ГСЧ для данного генераторного полинома.

Полученные результаты

Результаты исследования циклов ГСЧ на регистрах сдвиге с обратными связями, выполненных на модели рис.1, в объеме достаточном для понимания сути полученных результатов, приведены ниже. При этом для генераторных полиномов порядка 3 и 4 приведены и графы состояний и структура цикла, для m>4 структура циклов не указана. В связи с большим объемом материала по результатам исследований циклов, итоги исследований в полном объеме для m=(3…12) приведены тут: https://dl.dropboxusercontent.com/u/11291120/rezults.rar. Основные результаты исследований - генераторные полиномы, графы и структура циклов:

Порядок полинома: m = 3.

G(x) = x^3+1.	A(n):[0][1 2 4][3 6 5][7].	Г=2x3+2x1
G(x) = x^3+x+1.	A(n):[0][1 3 7 6 5 2 4].	Г=1x7+1x1
G(x) = x^3+x^2+1.	A(n):[0][1 2 5 3 7 6 4].	Г=1x7+1x1
G(x) = x^3+x^2+x+1	A(n):[0][1 3 6 4][2 5][7].	Г=1x4+1x2+2x1

Порядок полинома: m = 4.

G(x) = x^4+1.	A(n):[0][1 2 4 8][3 6 12 9][5 10][7 14 13 11][15].	Г=3x4+1x2+2x1
G(x) = x^4+x+1.	A(n):[0][1 3 7 15 14 13 10 5 11 6 12 9 2 4 8].	Г=1x15+1x1
G(x) = x^4+x^2+1.	A(n):[0][1 2 5 10 4 8][3 7 15 14 12 9][6 13 11].	Г=2x6+1x3+1x1
G(x) = x^4+x^2+x+1.	A(n):[0][1 3 6 13 10 4 8][2 5 11 7 14 12 9][15].	Г=2x7+2x1
G(x) = x^4+x^3+1.	A(n):[0][1 2 4 9 3 6 13 10 5 11 7 15 14 12 8].	Г=1x15+1x1
G(x) = x^4+x^3+x+1.	A(n):[0][1 3 7 14 12 8][2 4 9][5 10][6 13 11][15].	Г=1x6+2x3+1x2+2x1
G(x) = x^4+x^3+x^2+1.	A(n):[0][1 2 5 11 6 12 8][3 7 14 13 10 4 9][15].	Г=2x7+2x1
G(x) = x^4+x^3+x^2+x+1.	A(n):[0][1 3 6 12 8][2 5 10 4 9][7 15 14 13 11].	Г=3x5+1x1

Порядок полинома: m = 5.

G(x) = x^5+1.	Г=6x5+2x1
G(x) = x^5+x+1.	Г=1x21+1x7+1x3+1x1
G(x) = x^5+x^2+1.	Г=1x31+1x1
G(x) = x^5+x^2+x+1.	Г=1x14+2x7+1x2+2x1
G(x) = x^5+x^3+1.	Г=1x31+1x1
G(x) = x^5+x^3+x+1.	Г=2x15+2x1
G(x) = x^5+x^3+x^2+1.	Г=1x12+1x6+1x4+2x3+1x2+2x1
G(x) = x^5+x^3+x^2+x+1.	Г=1x31+1x1
G(x) = x^5+x^4+1.	Г=1x21+1x7+1x3+1x1
G(x) = x^5+x^4+x+1.	Г=2x8+3x4+1x2+2x1
G(x) = x^5+x^4+x^2+1.	Г=2x15+2x1
G(x) = x^5+x^4+x^2+x+1.	Г=1x31+1x1
G(x) = x^5+x^4+x^3+1.	Г=1x14+2x7+1x2+2x1
G(x) = x^5+x^4+x^3+x+1.	Г=1x31+1x1
G(x) = x^5+x^4+x^3+x^2+1.	Г=1x31+1x1
G(x) = x^5+x^4+x^3+x^2+x+1.	Г=4x6+2x3+2x1

Порядок полинома: m = 6.

G(x) = x^6+1.	Г=9x6+2x3+1x2+2x1
G(x) = x^6+x+1.	Г=1x63+1x1
G(x) = x^6+x^2+1.	Г=4x14+1x7+1x1
G(x) = x^6+x^2+x+1.	Г=2x31+2x1
G(x) = x^6+x^3+1.	Г=7x9+1x1
G(x) = x^6+x^3+x+1.	Г=1x28+1x14+2x7+1x4+1x2+2x1
G(x) = x^6+x^3+x^2+1.	Г=2x31+2x1
G(x) = x^6+x^3+x^2+x+1.	Г=4x15+1x3+1x1
G(x) = x^6+x^4+1.	Г=4x14+1x7+1x1
G(x) = x^6+x^4+x+1.	Г=2x21+2x7+2x3+2x1
G(x) = x^6+x^4+x^2+1.	Г=6x8+3x4+1x2+2x1
G(x) = x^6+x^4+x^2+x+1.	Г=3x21+1x1
G(x) = x^6+x^4+x^3+1.	Г=2x31+2x1
G(x) = x^6+x^4+x^3+x+1.	Г=1x63+1x1
G(x) = x^6+x^4+x^3+x^2+1.	Г=3x15+3x5+1x3+1x1
G(x) = x^6+x^4+x^3+x^2+x+1.	Г=1x30+2x15+1x2+2x1
G(x) = x^6+x^5+1.	Г=1x63+1x1
G(x) = x^6+x^5+x+1.	Г=3x10+6x5+1x2+2x1

G(x) = x^6+x^5+x^2+1.	Г=2x21+2x7+2x3+2x1
G(x) = x^6+x^5+x^2+x+1.	Г=1x63+1x1
G(x) = x^6+x^5+x^3+1.	Г=1x28+1x14+2x7+1x4+1x2+2x1
G(x) = x^6+x^5+x^3+x+1.	Г=4x12+2x6+1x3+1x1
G(x) = x^6+x^5+x^3+x^2+1.	Г=1x63+1x1
G(x) = x^6+x^5+x^3+x^2+x+1.	Г=2x31+2x1
G(x) = x^6+x^5+x^4+1.	Г=2x31+2x1
G(x) = x^6+x^5+x^4+x+1.	Г=1x63+1x1
G(x) = x^6+x^5+x^4+x^2+1.	Г=3x21+1x1
G(x) = x^6+x^5+x^4+x^2+x+1.	Г=3x12+1x6+3x4+2x3+1x2+2x1
G(x) = x^6+x^5+x^4+x^3+1.	Г=4x15+1x3+1x1
G(x) = x^6+x^5+x^4+x^3+x+1.	Г=2x31+2x1
G(x) = x^6+x^5+x^4+x^3+x^2+1.	Г=1x30+2x15+1x2+2x1
G(x) = x^6+x^5+x^4+x^3+x^2+x+1.	Г=9x7+1x1

Из приведенных здесь данных, характеризующих циклы, следует:

1. Мощность множества состояний регистра сдвига с обратными связями (число вершин графа), независимо от приводимости/неприводимости генераторного полинома равно $M = 2^m$, циклы разделяют это множество на непересекающиеся подмножества, что позволяет выполнять конкатенацию циклов заменой ВНЗ.

2. Минимальное число циклов у последовательностей, порожденных неприводимым генераторным полиномом, равно 2.

3. Число полиномов порядка m, пригодных для использования при создании ГСЧ на регистрах сдвига с обратными связями, определяется выражением (6).

Выводы

Выполненное исследование показало:

1. Применение конкатенации циклов ГСЧ на регистрах сдвига с обратными связями, независимо от приводимости/ неприводимости генераторного полинома степени m позволяет получить «склеенный» цикл (сверхцикл) длиной $M = 2^m$ слов.

2. Применение конкатенации сверхциклов, порожденных генераторными полиномами одной и той же степени m, позволяет «склеивать» сверхциклы и получить гиперцикл длиной $T = 2^{2m-1}$ слов.

3. В каждом из этих случаев ГСЧ на регистре сдвига с обратными связями, порождает равномерно распределенную последовательность чисел в интервале $\overline{(0,(M-1))}$ с нулевой ошибкой воспроизведения дискретной случайной величины, эта последовательность воспроизводима, а ее предсказуемость и степень корреляции слов последовательности существенно меньше общеизвестных ГСЧ этого класса, в то время как период повторения последовательности существенно больше.

Литература

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с. – (СКБ – специалисту по компьютерной безопасности).
2. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 822 с.
3. Кнут Д.Э. Искусство программирования: Получисленные алгоритмы / Кнут Д.Э. – М. : Вильямс, 2007. – Т. 2. – 832 с.

References

1. Michael Ivanov Theory, Application and evaluation of quality of Pseudorandom number generators / Ivanov, Chuhunkov. - Moscow: KUDITS-OBRAZ, 2003. - 240 p. - (SKB - Specialist in Computer Security).
2. Rudolf Lidl, Harald Niederreiter, Finite Fields - Moskow, 1988, 822 p
3. The Art of Computer Programming, 2: Seminumerical Algorithms (3rd ed.), Addison-Wesley Professional 1997. - 832 p.

Рецензія/Peer review : 29.10.2013 р. Надрукована/Printed :6.2.2014 р.
Рецензент: д.т.н., профессор Златкин А.А.