Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный университет имени Ф.М. Достоевского»

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра экспериментальной физики и радиофизики

Доклад

Генератор псевдослучайно последовательности чисел в широкополосной системе связи специального назначения.

Выполнил:

Студент 1ого курса

Группы ФРМ-302-О

Пихненко Олег Игоревич

Цель и задачи

Цель – программная реализация ГПСЧ для системы связи специального назначения.

Задачи:

- Анализ существующих ГПСЧ и выбор наиболее подходящего ГПСЧ для данной задачи.
- Программная реализация выбранного ГПСЧ.
- Тестирование полученных псевдослучайных последовательностей.

Некоторые ГПСЧ:

1. Регистр сдвига с линейной обратной связью.
2. Линейный конгруэнтный метод.
3. Вихрь Мерсенна.
4. BBS.
5. Алгоритм xor-shift.
6. Метод Фибоначчи.

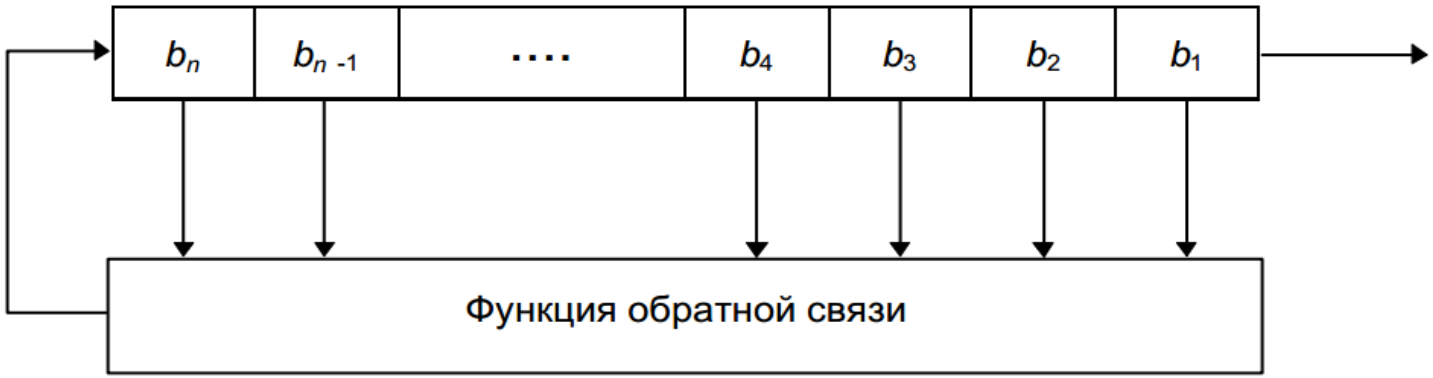


Рис.1. Сдвиговый регистр с обратной связью.

Сдвиговый регистр с обратной связью

Основные компоненты:

- Сдвиговый регистр
- Функция обратной связи

Преимущества:

•Высокое быстродействие

•Простота программной и аппаратной реализации

•Хорошие криптографические свойства

Сдвиговый регистр с линейной обратной связью

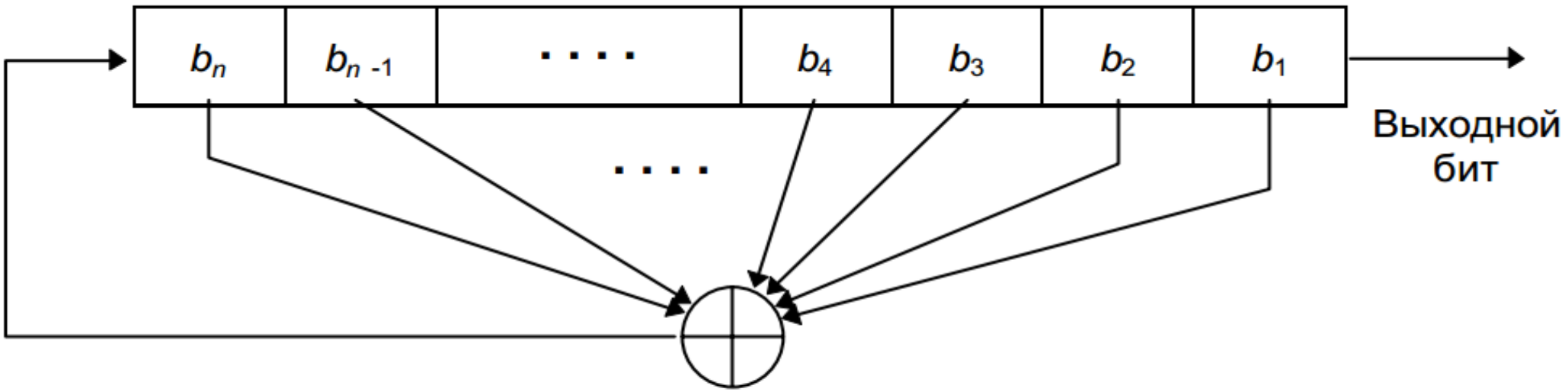


Рисунок 2. Сдвиговый регистр с линейной обратной связью (linear-feedback shift register или LFSR)

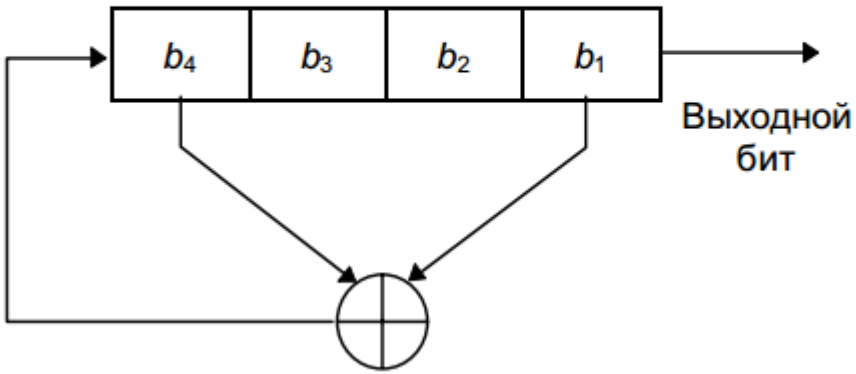
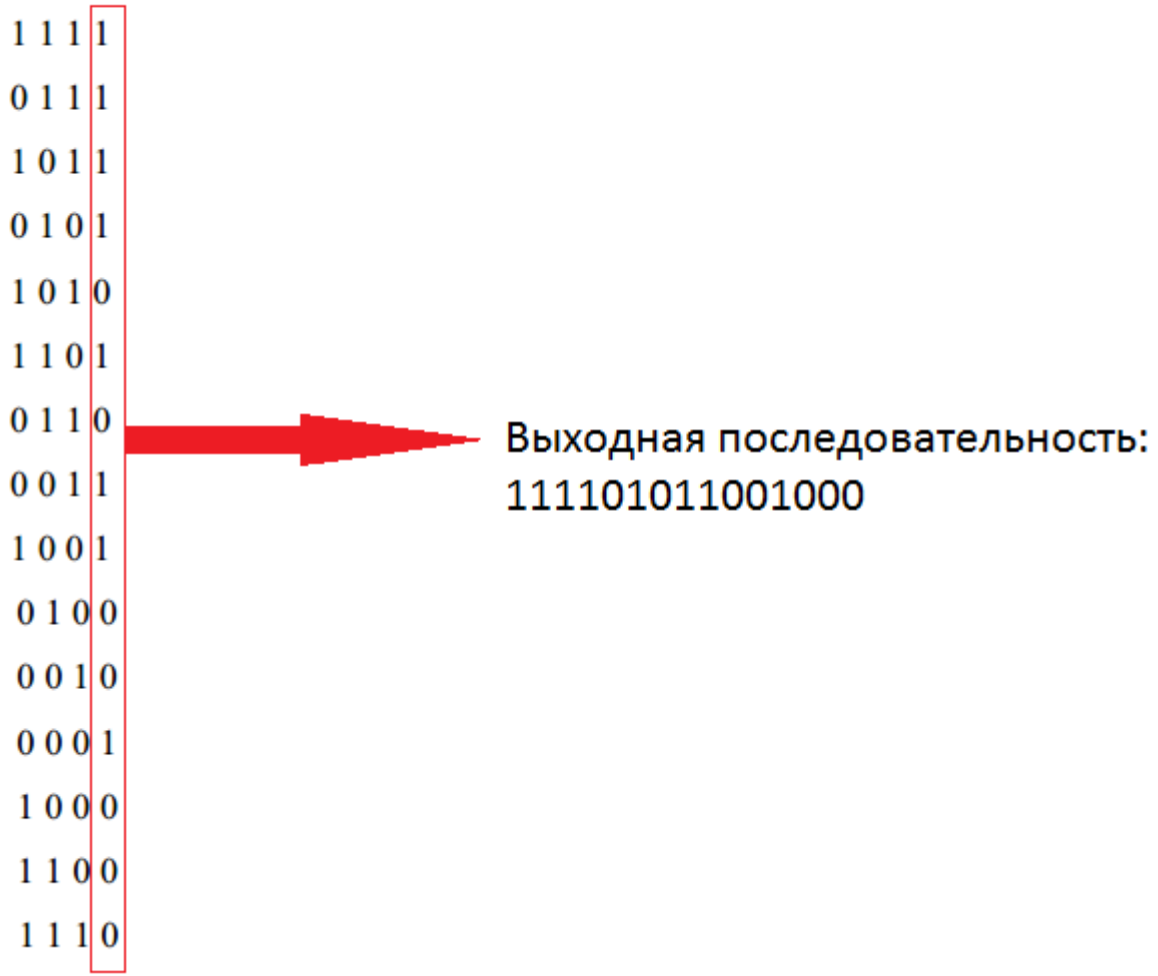


Рисунок 3. 4х битный LFSR, его внутренние состояния за один период работы и выходная последовательность.



Основные характеристики

- N-битовый LFSR может находиться в одном из (2^n)- 1 внутренних состояний.
- LFSR с максимальным периодом – это LFSR циклически проходящий все внутренние состояния.
- Только при определенных отводных LFSR может иметь максимальный период.
- Для того, чтобы конкретный LFSR имел максимальный период, многочлен, образованный из отводной последовательности и константы 1, должен быть примитивным по модулю 2. **Пример:** $x^{32}+x^{7}+x^{5}+x^{2}+x+1$.

Название теста	Статистика теста c(S)	Выявляемый дефект
Частотный тест	Нормализованная абсолютная сумма значений элементов последовательности	Слишком много нулей или единиц в последовательности
Частотный тест внутри блока	Мера согласования наблюдаемого количества единиц внутри блока с теоретически ожидаемым.	Локализованные отклонения частоты появления единиц в блоке от идеального значения ½.
Проверка накопленных сумм	Максимальное отклонение значения накопленной суммы элементов последовательности от начальной точки от-счета (точка 0)	Большое значение единиц или нулей вначале или в конце двоичной последовательности.
Проверка линейной сложности	Мера согласования наблюдаемого количества событий, заключающихся в появлении фиксированной длины эквивалентного ЛРР для заданного блока с теоретически ожидаемым.	Недостаточную сложность тестируемой последовательности.
Универсальный тест Маурера	Сумма логарифма расстояния между l-битными шаблонами.	Отклонение от теоретического закона распределения максимальных длин серий единиц.

Набор статических тестов “NIST STS”:

В 1999 году специалистами NIST, в рамках проекта AES (Advanced Encryptio Standard) был разработан набор статистических тестов NIST STS (NIST Statistical Test Suite) и предложена методика проведения статистического тестирования ГСЧ (ГПСЧ), которые на настоящий момент наилучшим образом отвечают потребностям всех заинтересованных сторон.

Порядок тестирования двоичной последовательности S

Выдвигается нулевая гипотеза H_0– предположение о том, что данная двоичная последовательность S случайна.

По последовательности S вычисляется статистика теста $c(S)$.

С использованием специальной функции и статистики теста вычисляется значение вероятности $P = f(c(S))$, $P \in [0, 1]$.

Значение вероятности P сравнивается с уровнем значимости α, $\alpha \in [0{,}001, 0{,}01]$. Если $P \geq \alpha$, то гипотеза H_0 принимается. В противном случае принимается альтернативная гипотеза.

Для осуществления тестирования были выбраны следующие параметры:

1. Длина тестируемой последовательности $n = 10^6$ бит.
2. Количество тестируемых последовательностей $m = 100$. Таким образом, объем тестируемой выборки составил $N = 10^6 \times 100 = 10^8$ бит.
3. Каждая последовательность генерировалась на основе различных отводных последовательностей и различных начальных значений инициализации регистра сдвига.
4. Уровень значимости $\alpha = 0{,}01$.

Название теста	p-value
Частотный (монобитный) тест	0.85335011
Частотный тест внутри блока	0.78190931
Проверка накопленных сумм	0.84519221
Проверка серий	0.78199317
Проверка максимальной длины серии в блоке	0.6054288
Проверка ранга двоичной матрицы	0.94179309
Спектральный тест на основе дискретного преобразования Фурье	0.85721388
Проверка перекрывающихся шаблонов	0.09568771
Универсальный тест Маурера	0.68037894
Энтропийный тест	0.12327079
Проверка случайных отклонений	0.85335011
Проверка случайных отклонений (вариант)	0.74103231
Последовательный тест	0.97480684
Проверка сжатия по алгоритму Лемпеля-Зива	0.77966582
Проверка неперекрывающихся шаблонов	0.60761019
Проверка линейной сложности	0.76054288

Результат

- Все тесты показали значение p больше уровня значимости.

Литература:

1. Д. Кнут. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т.2. – М.:Мир, 1977. – 700 с.
2. Б. Шнайер "Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си“ – Триумф, 2002. - 816 с.
3. В. Романьков “Введение в криптографию.” – Форум.
4. J.A. Gordon, “Very Simple Method To Find the Minimal Polynomial of an Arbitrary Non Zero Element of a Finite Field” Electronic Letters, 1976. – 663с.