Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ (КНИТУ-КАИ)

ЭФФЕКТИВНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННЫЙ НА НЕЧЕТКОЙ ЛОГИКЕ

05.13.18 - «Математическое моделирование, численные методы и комплексы программ»

Соискатель:
Альнаджар Халед Хасан
аспирант кафедры систем информационной безопасности (СИБ) КНИТУ-КАИ

Научный руководитель:
Аникин Игорь Вячеславович
к.т.н., доцент каф. СИБ КНИТУ-КАИ

2017

Цель диссертационной работы

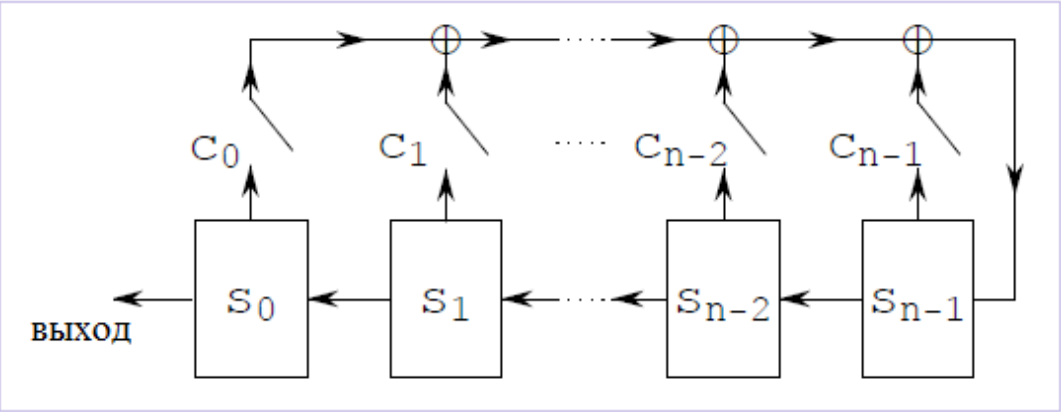
Повышение эффективности генерации псевдослучайных последовательностей за счет применения аппарата нечеткой логики в ГПСЧ.

Под эффективностью понимаются удовлетворение статистическим критериям качества.

Решаемые в работе задачи

1. Исследование методов построения ГПСЧ, в частности построенных на базе регистров сдвига с линейной обратной связью (РСЛОС).
2. Разработка архитектуры нового ГПСЧ, основанного на применении РСЛОС и нечеткой логики (НГПСЧ).
3. Исследование и выбор методов тестирования псевдослучайных последовательностей.
4. Исследование разработанной архитектуры НГПСЧ и выбор лучших значений параметров.
5. Оценка качества сгенерированных НГПСЧ последовательностей и сравнение НГПСЧ с другими известными генераторами.

ГПСЧ на основе регистров сдвига с линейной обратной связью (РСЛОС)



$$s_{k+n} = \sum_{i=0}^{n-1} c_i \, s_{k+i}, \qquad k \geq 0$$

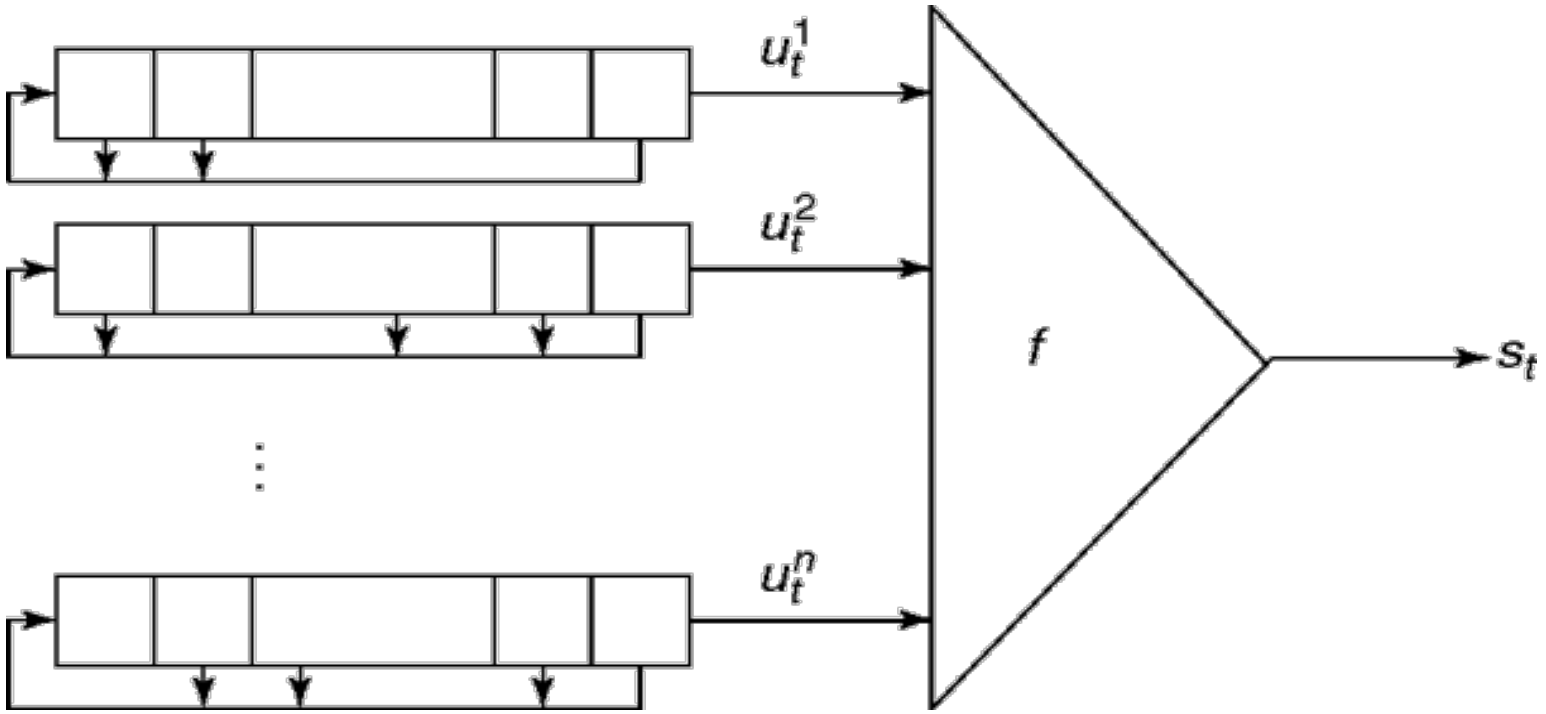
Преимущества использования РСЛОС

1. Высокое быстродействие.
2. Хорошие статистические свойства ПСЧ.
3. Возможность простой реализации на аппаратном уровне.

Недостатки использования РСЛОС

1. Линейность последовательности на выходе регистра.
2. Относительная лёгкость анализа РСЛОС с помощью алгоритма Берлекэмпа — Мэсси или алгоритма Евклида (возможность однозначного определения многочлена обратной связи по 2n последовательным битам).

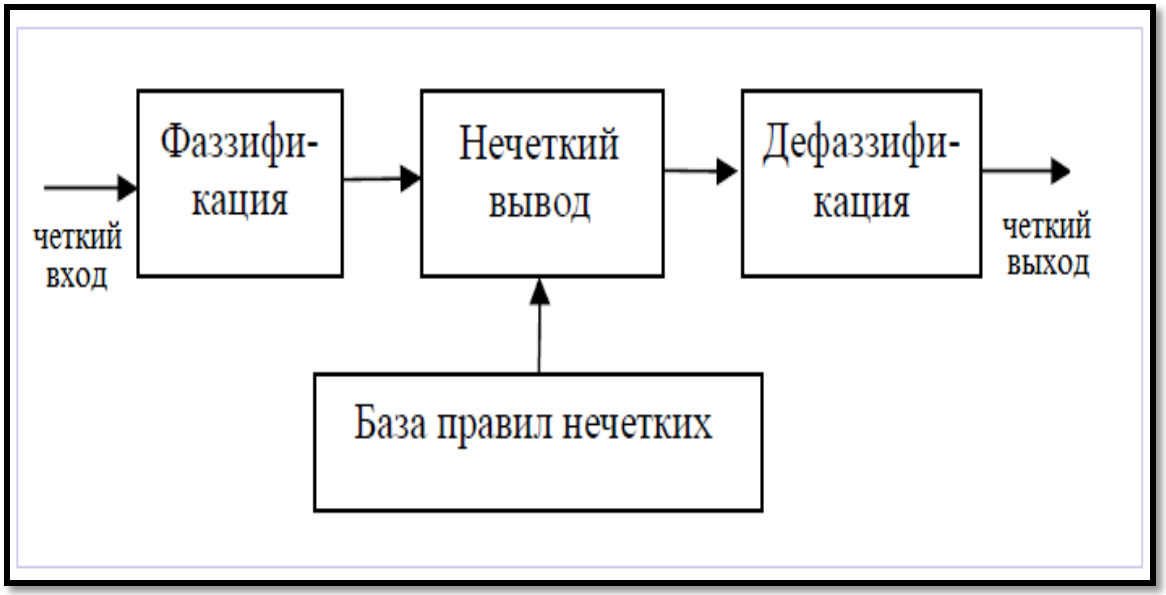
ГПСЧ на основе регистров сдвига с линейной обратной связью (РСЛОС)



Комбинация (РСЛОС) с применением нелинейной функции

Нелинейная функция строится на основе анализа статистических свойств выходов РСЛОС с применением нечеткой логики.

Общая структура системы нечеткого управления

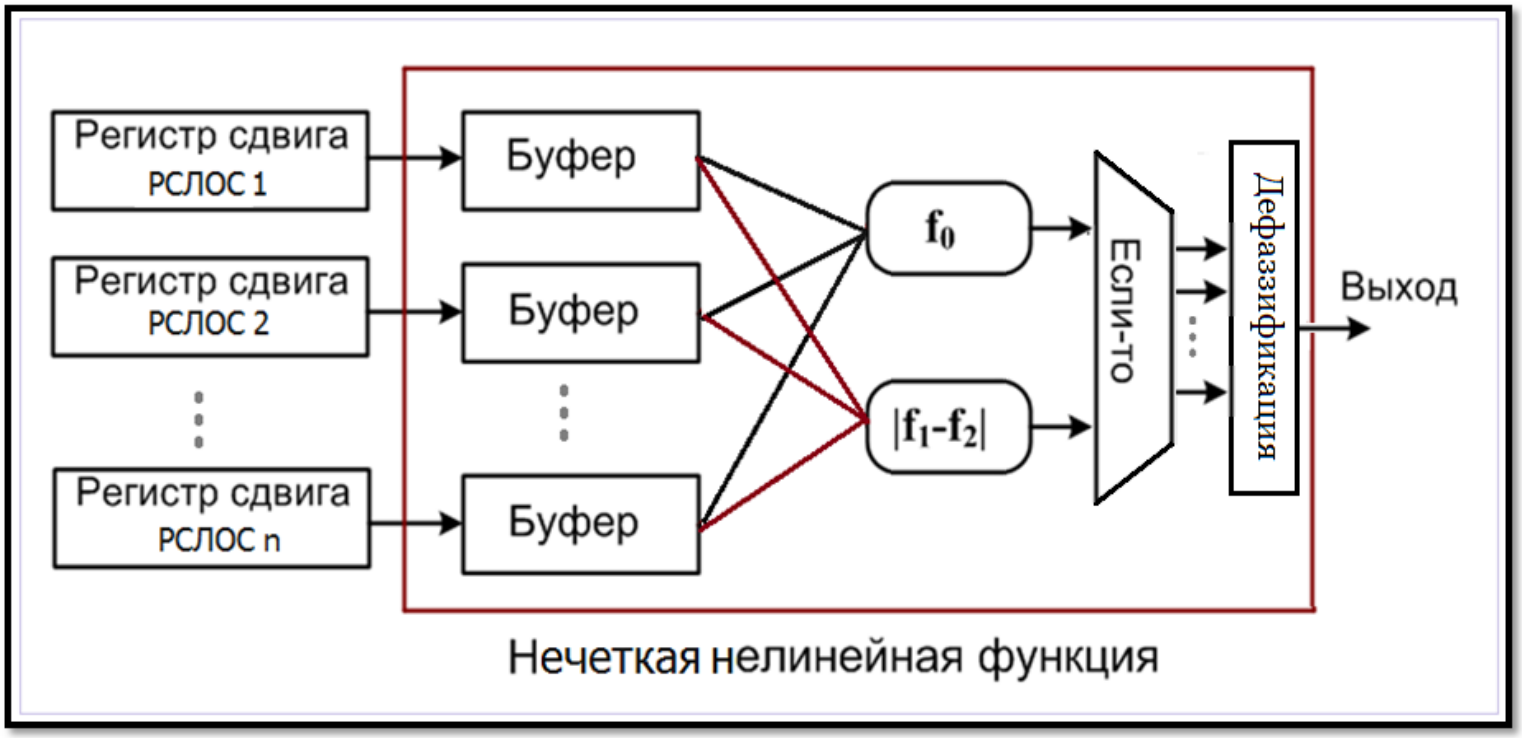


Преимущества использования нечеткой логики

1.Системы нечеткого логического вывода имеют множество свойств, полезных для использования в рассматриваемой области.

2.Применение нечеткой логики повышает линейную сложность построенного ГПСЧ.

Архитектура предложенного НГПСЧ



Предложенная архитектура включает в себя несколько регистров сдвига (РСОЛС), выходы которых поступают в буферы (8 бит).

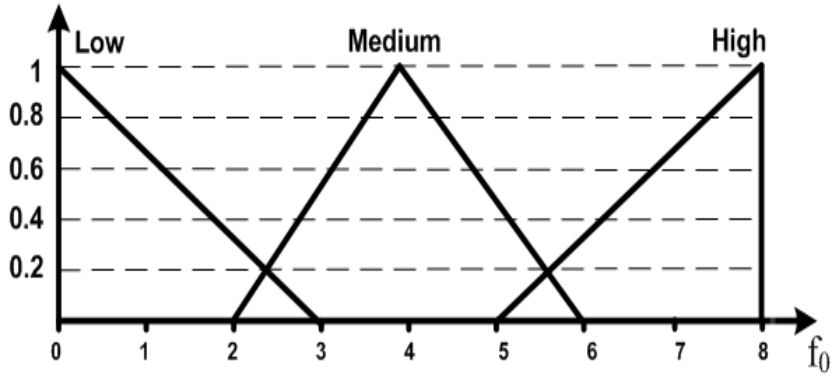
Далее производится оценка двух лингвистических переменных:

- количество единиц в буфере (f_0);
- разность между числом блоков (f_1) состоящих из двух единиц (0110) и количество пробелов (f_2) состоящих из двух нулей (1001) в каждом буфере $|f_2-f_1|$.

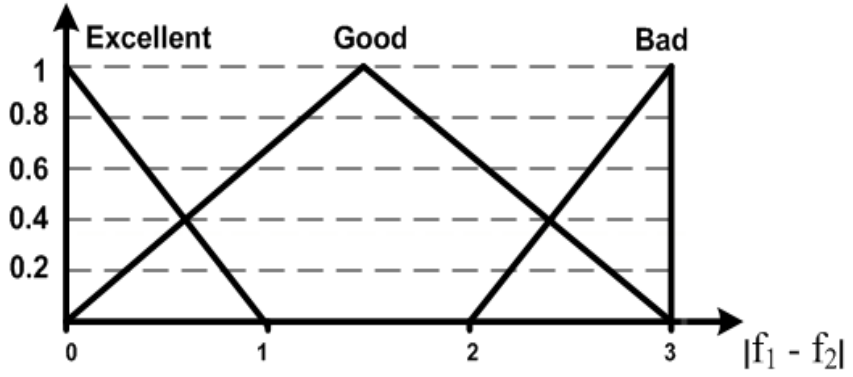
Архитектура предложенного НГПСЧ

Функции принадлежности лингвистических переменных f_0, $|f_2-f_1|$:

f_0 с тремя термами {Low, Medium, High}:
- {Low}, когда $f_0 \in \{0,1,2\}$;
- {Medium}, когда $f_0 \in \{3,4,5\}$;
- {High}, когда $f_0 \in \{6,7,8\}$.



$|f_2-f_1|$ с тремя термами {Excellent, Good, Bad}:
- {Excellent}, когда $|f_2-f_1| \in \{0\}$;
- {Good}, когда $|f_2-f_1| \in \{1,2\}$;
- {Bad}, когда $|f_2-f_1| \in \{3\}$.



Архитектура предложенного НГПСЧ

Набор нечетких правил ЕСЛИ-ТО правил генератора НГПСЧ представлен в таблице

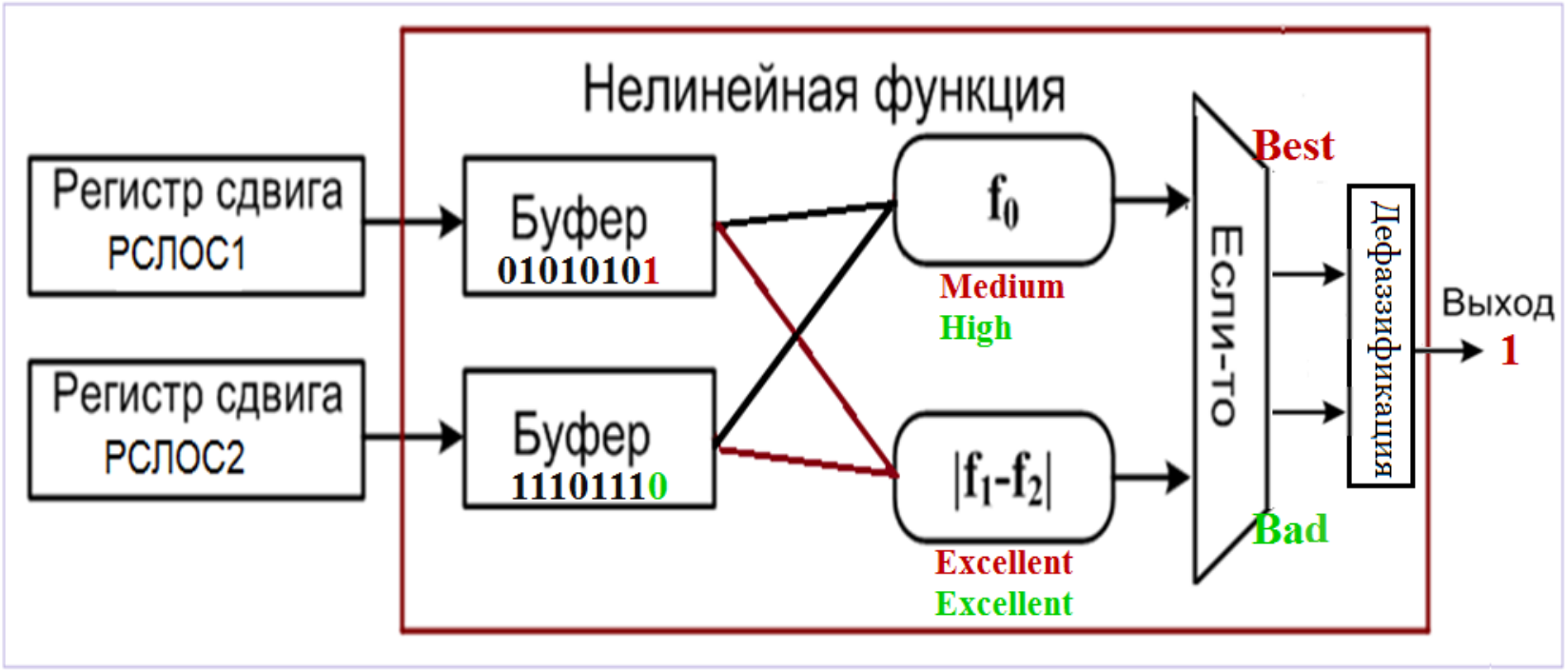
f_0 / $\lvert f_1-f_2 \rvert$	*Low*	*Medium*	*High*
Excellent	Bad	Best	Bad
Good	Good	Good	Good
Bad	Bad	Good	Bad

Оператор дефаззификации представлен в следующей таб.

LFSR1 / LFSR2	Best	Good	Bad
Best	Bit2	Bit2	Bit2
Good	Bit1	Bit2	Bit2
Bad	Bit1	Bit1	Bit2

В таблице (Bit1, Bit2) относятся к выходу РСОЛС1 и РСОЛС2 соответственно.

Пример



РСОЛС1: f_0 (01010101)=4 → (Medium)
РСОЛС1: $|f_2$ (01010101) - f_1 (01010101)|=|0-0|=0 → (Excellent) } **Best**
РСОЛС2: f_0(11101110)=6 → (High)
РСОЛС2: $|f_2$ (11101110) - f_1(11101110)|=|0-0|=0 → (Excellent) } **Bad**

→ **РСОЛС1 лучший**

Выход = 1

Требования к качественному ГПСЧ

С целью получения последовательностей очень близких к истинно случайным, ГПСЧ должен обладать следующими свойствами:

- обеспечивать большой период для сгенерированных псевдослучайных последовательностей;
- иметь хорошие статистические свойства (успешно проходить статистические тесты случайности НИСТ и DIEHARD);
- высокое быстродействие, диффузионную ёмкость, низкое энергопотребление;
- непредсказуемость;
- стойкость к алгебраическим атакам.

Исследование параметров НГПСЧ

С целью удовлетворения всех требований к качественным ГПСЧ, необходимо исследовать все параметры предложенного НГПСЧ, которые можно разделить на две группы.

Параметры первой группы (параметры РСЛОС)

- Период сгенерированной последовательности (Ts).
- Характеристический полином РСЛОС.

Параметры второй группы (параметры нелинейной функции на основе нечеткой логики)

Данные параметры непосредственно влияют на случайность полученной последовательности:

- объём буфера;
- количество термов каждой из лингвистических переменных;
- совокупность правил ЕСЛИ-ТО;
- тип функций принадлежности;
- функции принадлежности линвистических переменных.

Исследование периода сгенерированной последовательности (T_s)

Выбраны два простых примитивных полинома над полем Галуа F_2 для упрощения исследования и определения того, как относится T_s к периодам используемых регистров РСЛОС$_1$ (T_1) и РСЛОС$_2$ (T_2).

$$P_1(x) = 1 + x^3 + x^5$$

$$P_2(x) = 1 + x^6 + x^7$$

Период каждого регистра определяется по формуле:

$$(T = 2^{degree} - 1)$$

Итак $T_1 = 2^5 - 1 = 31$, $T_2 = 2^7 - 1 = 127$

В результате исследования получено:

$$T_s = 3937 = 31 * 127 = T_1 * T_2$$

$$T_s = T_1 * T_2$$

Выбор характеристических примитивных полиномов РСЛОС

Вначале выбрано два примитивных полинома над полем Галуа F_2 для проверки удовлетворения первому постулату Голомба $T_s > 10^{50}$.

$$P_1(x)=1+x^{83}+x^{84}+x^{86}+x^{89},\ T_1=2^{89}-1=6.1897\times10^{26}$$
$$P_2(x)=1+x^{91}+x^{97},\ T_2=2^{97}-1=1.58456\times10^{29}$$
$$T_s=T_1\cdot T_2=\ 9.80797\times10^{55}\geq10^{50}$$

Далее проведено исследование случайности сгенерированных НГПСЧ последовательностей с помощью пакета статистических тестов НИСТ. Данный пакет включает в себя 15 статистических тестов, которые разработаны для проверки гипотезы о случайности двоичных последовательностей, порождаемых ГСЧ или ГПСЧ.

НГПСЧ успешно прошел все тесты пакета НИСТ.

характеристический примитивный полином РСЛОС имеет значительное влияние на следующие свойства ГПСЧ:

- статистические свойства генерированной последовательности;
- безопасность и стойкость генератора;
- эффективность генератора (высокую диффузионную ёмкость, высокую производительность и минимальные затраты на аппаратную реализацию).

Характеристический полином РСЛОС должен иметь:

- высокую степень (длинный период);
- большой вес Хэмминга ≥ 10 (высокую диффузионную ёмкость);
- минимальные затраты на аппаратную реализацию (минимальное логических элементов XOR(исключающее ИЛИ)).

Нам нужно найти компромиссное решение

Достаточно хорошее решение данной проблемы предложено в статье Laung-Terng Wang, Nur A. Touba, Richard P. Brent,Hui Xu, and Hui Wang. November 8, 2011. “On Designing Transformed Linear Feedback Shift Registers with Minimum Hardware Cost”.

$$f(x) = (1 + x^{b_1}) \cdot (1 + x^{b_2}) \cdots (1 + x^{b_m}) + x^n$$

$$b_1 \geq 1, \quad b_1 < b_2, \quad (b_1 + b_2) < b_3, \ldots, (b_1 + b_2 + \cdots + b_{m-1}) < b_m, \ (b_1 + b_2 + \ldots + b_m) < n$$

мы выбрали m=5, вес Хэмминга $W=2^m+1=32+1=33$.

Преимущества полиномов данного типа

- Имеет большой вес Хэмминга = 33 (высокую диффузионную ёмкость);
- Минимальные затраты на аппаратную реализацию (минимальное количество логических элементов XOR = 5).

Поиск примитивных полиномов для НГПСЧ

Был написан алгоритм и создана программа в пакете "*Mathematica*" для нахождения списка примитивных полиномов данного типа со степенями n от 35 до 200.

Данные примитивные полиномы выбраны для разработанного НГПСЧ:

$$P_1(x) = (1+x)\cdot(1+x^5)\cdot(1+x^{10})\cdot(1+x^{17})\cdot(1+x^{39})+x^{89}$$

$$P_2(x) = (1+x)\cdot(1+x^4)\cdot(1+x^7)\cdot(1+x^{20})\cdot(1+x^{53})+x^{97}$$

Параметры второй группы

Параметры нелинейной функции НГПСЧ непосредственно влияют на случайность полученной последовательности, к этой группе относятся:

- объём буфера;
- количество термов каждой нечеткой переменной;
- совокупность правил ЕСЛИ-ТО;
- тип функций принадлежности;;
- функции принадлежности линвистических переменных.

Объём буфера

Исследовалось 5 возможных значений (8,16,24,32,64) с целью нахождения наилучшего из них.

Количество термов каждой нечеткой переменной

Исследовалось три значения (3,5,7) для первой лингвистической переменной f_0 и два значения (3,5) для второй линвистической переменной $|f_2-f_1|$ имеет два значения (3,5). Всего - 3x2 = 6 ситуаций

$(f_0 , |f_2-f_1|) = \{(3,3),(3,5),(5,3),(5,5),(7,3),(7,5)\}$.

Совокупность правил Если-То

Данный параметр влияет на статистические свойства сгенерированной последовательности. Количество правил пропорционально зависит от двух количества значений лингвистических переменных. Например: когда $(f_0, |f_2-f_1|) = (5,3)$, то |Если-То|=13.

f_0 / $\|f_2-f_1\|$	Very Low	Low	Medium	High	Very High
Excellent	Bad	Good	Best	Good	Bad
Good	Bad	Bad	Good	Bad	Bad
Bad	X	Bad	Good	Bad	X

Исследование параметров второй группы

Нам нужно сгенерировать, протестировать и сравнить 6*5=30 последовательностей, чтобы определить наилучшие значений исследуемых параметров.

Тесты псевдослучайных последовательностей (ПСП)

Тесты ПСП разделяются на две группы: эвристические и статистические. Эвристические тесты дают относительную оценку нескольких альтернативных генераторов (по отношению друг к другу) , а статистические тесты ищут в ПСП детерминированную составляющую и дают абсолютную оценку качества генератора.

Эвристические тесты	Статистические тесты
❑ проверка скорости; ❑ проверка периода; ❑ на точность определения неких констант (например, числа Пи) методом Монте-Карло; ❑ прочие.	❑ равномерность распределения; ❑ независимость элементов числовой последовательности; ❑ совпадение числовых характеристик; ❑ комплексные критерии, которые проверяют сразу несколько вышеуказанных требований.

Для исследования предложенного НГПСЧ использованы два пакета статистических тестов на случайность: НИСТ и DIEHARD, а также метод Монте-Карло.

Пакет статистических тестов НИСТ

Пакет НИСТ включает в себя 15 статистических тестов, которые разработаны для проверки гипотезы о случайности двоичных последовательностей, порождаемых ГПСЧ. Все тесты направлены на выявление различных дефектов случайности.

Список пакета тестов НИСТ

1. Частотный побитовый (монобитный) тест;
2. Частотный тест внутри блока;
3. Тест на последовательность одинаковых битов;
4. Тест на самую длинную последовательность единиц в блоке;
5. Тест рангов бинарных матриц;
6. Спектральный тест;
7. Проверка неперекрывающихся шаблонов;
8. Проверка перекрывающихся шаблонов;
9. Универсальный статистический тест Маурера;
10. Тест на линейную сложность;
11. Последовательный тест;
12. Тест приблизительной энтропии;
13. Тест кумулятивных сумм;
14. Тест на произвольные отклонения;
15. Другой тест на произвольные отклонения.

В каждом тесте вычисляется одно или несколько значений $P\text{-}value \in [0,1]$.

Если $P\text{-}value \leq \alpha$ (уровень значимости), то последовательность не прошла соответствующий тест.

Методика тестирования ПСП с помощью НИСТ

1. Сформировать двоичную последовательность *S*;
2. Разделить последовательность *S* на множество из *m* подпоследовательностей;
3. Протестировать каждую подпоследовательность с использованием тестов пакета НИСТ. В результате сформировать таблицу значений P-values;
4. Произвести статистический анализ полученных результатов;
5. Принять окончательное решение о прохождении теста с помощью статистических критериев качества.

Критерии принятия решения о прохождении теста

1. Получение средних значений и дисперсии P-values, дальнейшее их сравнение со средним значением (0.5) и дисперсией (1/12) равномерного распределения;
2. Критерий хи-квадрат с девятью степенями свободы;

интервал [0,1] разбивается на 10 равных частей $\chi_j^2 = \sum_{k=1}^{10} \frac{(f_k - m/10)^2}{m/10}$

$$P_\vartheta\left(\chi^2_{\text{эксп}}\right) = igamc\left(\frac{9}{2}, \frac{\chi^2_{\text{эксп}}}{2}\right) \geq 0.0001 \iff \chi^2_{\text{эксп}} \leq 29.6$$

3. Отношение числа неудачных последовательностей к общему числу тестируемых последовательностей.

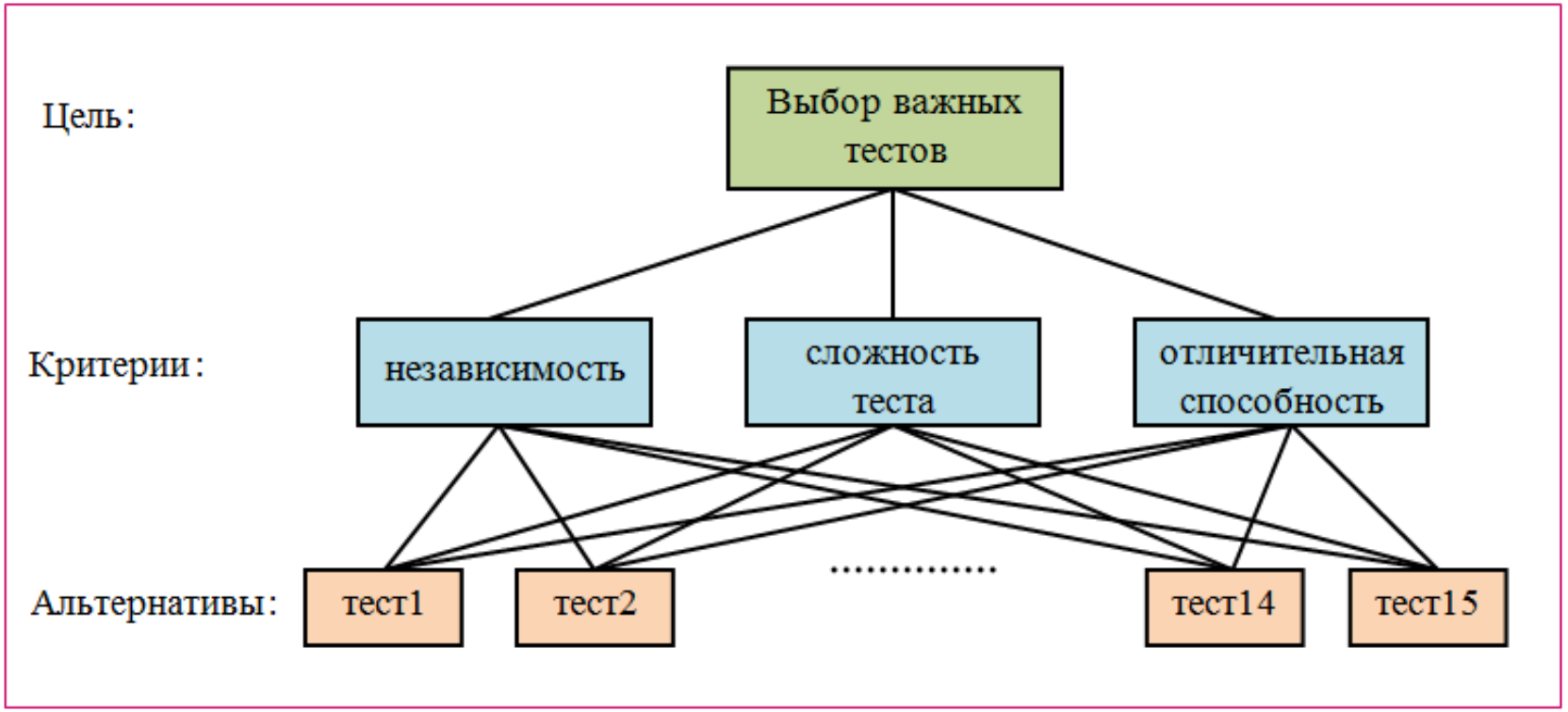
Для каждого теста определятся параметр r_j где j ∈ {1,2,…,15}

$$r_j = \frac{\#\{P_{i,j} \geq \alpha \mid i = 1,\dots,m\}}{m} \in r_{\max(\min)} = \hat{P} \pm 3\sqrt{\frac{\hat{P}(1-\hat{P})}{m}} \Bigg\} \iff \eta_{Accept} = 19.4,$$
$$\hat{P} = 1 - \alpha$$

где α = 0.01 & m=1000

Метод анализа иерархий (МАИ) для выбора важнейших тестов пакета НИСТ

Метод анализа иерархий (МАИ) был использован для выбора наиболее важных статистических тестов из набора статистических тестов НИСТ, с целью сокращения времени тестирования.



Метод анализа иерархий (МАИ) для выбора важнейших тестов пакета НИСТ

Результаты применения метода МАИ показаны в следующей таблице

Название теста	глобальный приоритету	Порядок важности
1. Частотный побитовый (монобитный) тест	0.1051	**2**
2. Частотный тест внутри блока	0.0731	**5**
3. Тест на последовательность одинаковых битов	0.0977	**3**
4. Тест на самую длинную последовательность единиц в блоке	0.1476	**1**
5. Тест рангов бинарных матриц	0.0655	6
6. Спектральный тест	0.0552	10
7. Проверка неперекрывающихся шаблонов	0.0447	11
8. Проверка перекрывающихся шаблонов	0.0614	7
9. Универсальный статистический тест Маурера	0.0206	15
10. Тест на линейную сложность	0.0459	12
11. Последовательный тест	0.0571	9
12. Тест приблизительной энтропии	0.0966	**4**
13. Тест кумулятивных сумм	0.0394	13
14. Тест на произвольные отклонения	0.0592	8
15. Другой тест на произвольные отклонения	0.0360	14

Исследование параметров НГПСЧ
Объём буфера, Количество термов и Если-То правил

Тестировалось 30 последовательностей длиной 1024000 бит, каждая из которых была разделена на 1000 подпоследовательностей длиной 1024 бита. К ним были применены выбранные 5 наиболее важных статистических тестов пакета НИСТ.

Результаты применения первой критерии (среднее значение и дисперсия):

количество термов f_0, $\lvert f_1-f_2\rvert$	объём буфера	T1	T2	T3	T4	T5
3, 3	8	+	-	-	+	-
	16	+	+	+	+	+
	24	+	+	+	+	+
	32	+	+	+	+	+
	64	+	+	+	+	+
5, 3	8	+	-	-	+	-
	16	+	-	+	+	+
	24	+	-	+	+	+
	32	-	-	+	+	+
	64	+	-	+	+	+
7, 3	8	+	-	-	+	-
	16	+	-	+	+	+
	24	+	-	+	+	+
	32	+	-	+	+	+
	64	+	-	+	+	+
3, 5	16	+	-	+	+	+
	24	+	-	+	+	+
	32	+	+	+	+	+
	64	+	+	+	+	+
5, 5	16	+	-	+	+	+
	24	+	-	+	+	+
	32	+	-	+	+	+
	64	+	+	+	+	+
7, 5	16	+	-	+	+	+
	24	+	-	+	+	+
	32	+	-	+	+	+
	64	+	-	+	+	+

Результаты применения второго критерия оценки качества (хи-квадрат с девятью степенями свободы)

$$P_{\vartheta}\left(\chi^2_{\text{эксп}}\right) = igamc\left(\frac{9}{2}, \frac{\chi^2_{\text{эксп}}}{2}\right) \geq 0.0001 \quad \Longrightarrow \quad \chi^2_{\text{эксп}} \leq 29.6$$

количество термов f_0, $\lvert f_1 - f_2 \rvert$	объём буфера	T1	T2	T3	T4	T5
3, 3	16	+	-	+	+	+
	24	+	+	+	+	+
	32	+	+	+	+	+
	64	+	+	+	+	+
3, 5	32	-	+	+	+	+
	64	-	+	+	-	+
5, 5	64	-	-	+	+	+

Результаты применения третьего критерия оценки качества

$\eta_{Accept} < 19{,}4$ *per 1000*

Кол. термов f_0, $\lvert f_1 - f_2 \rvert$	объём буфера	T1	T2	T3	T4	T5	∑
3, 3	24	+ 9	+ 7	+ 11	- 21	+ 12	60
	32	+ 5	+ 9	+ 9	+ 5	+ 5	33
	64	+ 15	+ 13	+ 10	+ 6	+ 18	62

В результате исследования выявлено:

Размер буферов = 32 является лучшим вариантом, так как имеет меньшее число неудачных подпоследовательностей. Кроме этого данный вариант более предпочтительный с точки зрения практической реализации, так как требует меньше памяти, чем размер буфера = 64.

Результаты исследования параметров НГПСЧ (Объём буфера, Количество термов и ЕСЛИ-ТО правила)

В результате исследования определены наилучшие значения данных параметров:

- Объём буфера = 32;
- количество термов (f_0 , $|f_2-f_1|$) = (3,3);
- совокупность ЕСЛИ-ТО правил.

f_0 / $\lvert f_1-f_2 \rvert$	*Low*	*Medium*	*High*
Excellent	**Bad**	**Best**	**Bad**
Good	**Bad**	**Good**	**Bad**
Bad	**Bad**	**Bad**	**Bad**

Исследования параметров НГПСЧ (тип функций принадлежности)

Существует много типовых форм кривых для задания функций принадлежности. Наибольшее распространение получили: кусочно-линейные, Z-образные и S-образные, П-образные функции. С целью нахождения наилучшего варианта функций принадлежности нами рассматривались:

- треугольная ФП;
- трапециевидная ФП;
- ФП в виде функции плотности нормального распределения.

В результате исследования было выявлено, что трапециевидная функция принадлежности является наилучшим вариантом.

Стоит отметить, что данный параметр не имел большого влияния на качество формируемой выходной последовательности.

Исследование параметров НГПСЧ (функции принадлежности лингвистических переменных)

Данный параметр сильно влияет безопасность генератора. При построении нелинейных функций они должны удовлетворять критериям стойкости: обладать высокой нелинейностью, быть сбалансированными (стойкими по отношению к корреляционным атакам - КА). КА используют некоторые слабости в комбинирующей функции, которые позволяют по выходной последовательности получить информацию об отдельных входных последовательностях.

сбалансированная последовательность имеет:

$$P(out_{sys}=out_{LFSR2}) = P(out_{sys}=out_{LFSR1}) \cong 0.5$$

В нашей ситуации (до изменения):

- $P(out_{sys}=out_{LFSR1}) = 0.44$
- $P(out_{sys}=out_{LFSR2}) = 0.56$

С целью улучшения баланса сгенерированных последовательностей генератором НГПСЧ, данный параметр исследовался и подбиралось наилучшее значение.

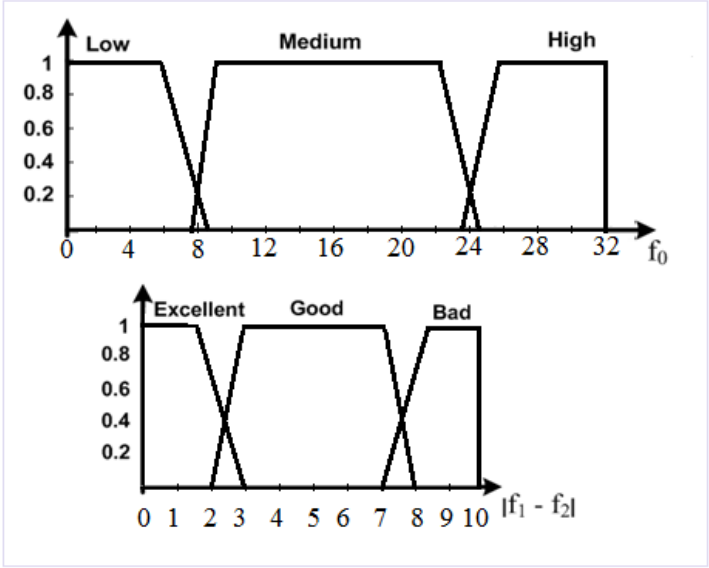
Исследование параметров НГПСЧ
(функции принадлежности лингвистических переменных)

Данный параметр сильно связен с предыдущим параметром (количество термов). Очевидно, что количество элементов подмножества каждой из лингвистических переменных имеет большое влияние на статистические свойства сгенерированной последовательности.

Начальные конфигурации подмножества каждой из лингвистических переменных НГПСЧ:

f_0 с тремя термами {Low, Medium, High}:
- {Low}, когда $f_0 \in \{0,1,2\}$;
- {Medium}, когда $f_0 \in \{3,4,5\}$;
- {High}, когда $f_0 \in \{6,7,8\}$.

$|f_2-f_1|$ с тремя термами {Excellent, Good, Bad}:
- {Excellent}, когда $|f_2-f_1| \in \{0\}$;
- {Good}, когда $|f_2-f_1| \in \{1,2\}$;
- {Bad}, когда $|f_2-f_1| \in \{3\}$.



Замечание: эти конфигурации общие для двух буферов (РСЛОС1, РСЛОС2).

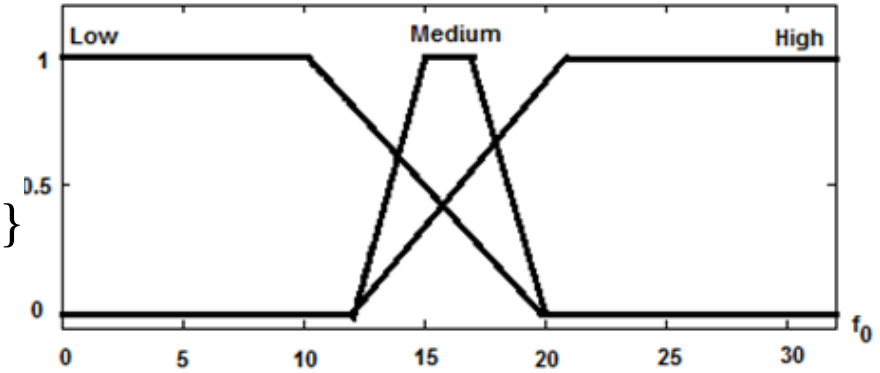
Исследование параметров НГПСЧ (функции принадлежности лингвистических переменных)

В результате исследования данного параметра была найдена наилучшая конфигурация лингвистических переменных для каждого из используемых регистров (РСЛОС1, РСЛОС2):

1. Для первого регистра РСЛОС1

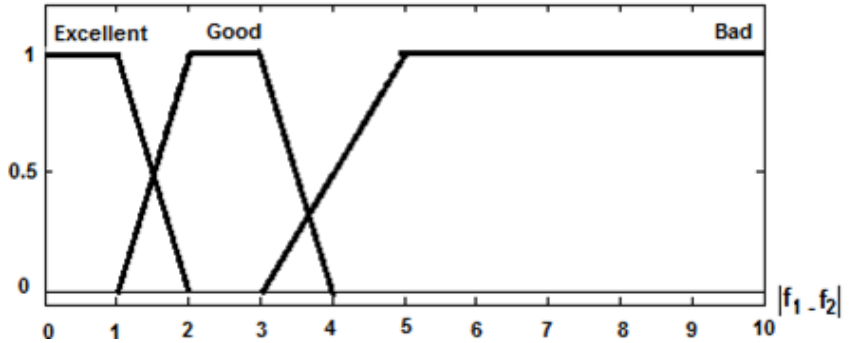
f_0 с тремя лингвистическими термами {Low, Medium, High}:

- когда $f_0 \in \{0,...,13\}$ назначается {Low};
- когда $f_0 \in \{14,...,17\}$ назначается {Medium}
- когда $f_0 \in \{18,...,32\}$ назначается {High}.



$|f_2-f_1|$ с тремя лингвистическими термами {Excellent, Good, Bad}:

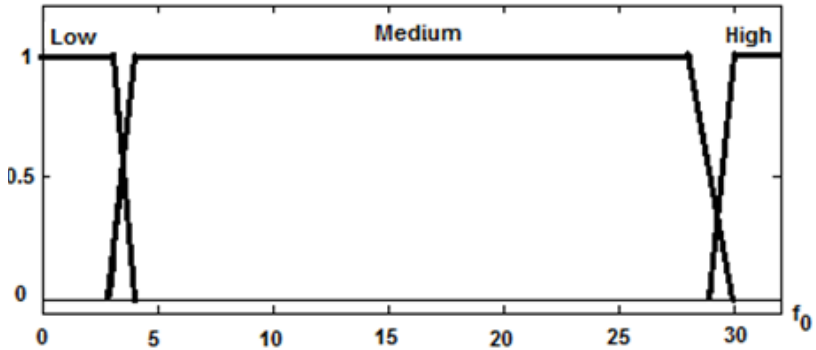
- когда $|f_2-f_1| \in \{0,1\}$ назначается {Excellent}
- когда $|f_2-f_1| \in \{2,3\}$ назначается {Good};
- когда $|f_2-f_1| \in \{4,...,10\}$ назначается {Bad}.



Исследование параметров НГПСЧ (функции принадлежности лингвистических переменных)

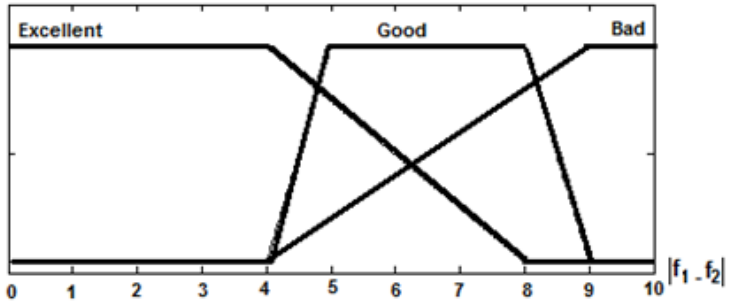
2. Для второго регистра РСЛОС2 f_0 с тремя лингвистическими термами {Low, Medium, High}:

- когда $f_0 \in \{0,...,3\}$ назначается на {Low};
- когда $f_0 \in \{4,...,28\}$ назначается на {Medium};
- когда $f_0 \in \{29,...,32\}$ назначается на {High}.



$|f_2-f_1|$ с тремя лингвистическими термами {Excellent, Good, Bad}:

- когда $|f_2-f_1| \in \{0,...,4\}$ назначается на {Excellent};
- когда $|f_2-f_1| \in \{5,...,8\}$ назначается на {Good};
- когда $|f_2-f_1| \in \{9,10\}$ назначается на {Bad}.



Замечание: полученные результаты показывают что, для каждого РСЛОС особенние конфигурации. Это значит что предложная архитектура действительно имеет 4 лингивических переменых по 2 для каждого РСЛОС.

Исследование параметров НГПСЧ (функции принадлежности лингвистических переменных)

Для подтверждения данных результатов проведено несколько вычислительных экспериментов с изменением количества сгенерированных битов и вычислением вероятности $P(out_{sys}=out_{LFSR2})$. Полученные результаты представлены в следующей таблице

количество генерируемых битов	**$P(out_{sys}=out_{LFSR2})$**
1000	0,5070
10000	0,5002
100000	0,4993
10000000	0,5000

Сгенерированные последовательности генератором НГПСЧ стали более сбалансированными после внесенных изменений.

Тестирование качества НГПСЧ

Для тестирования качества полученного НГПСЧ было проведено исследование сгенерированных последовательностей с помощью пакета тестов НИСТ. Сгенерирована последовательность с длиной 1024000 бит, которая разделена на 1000 подпоследовательностей длиной 1024 бита. К данным подпоследовательностям были применены 5 наиболее важных статистических тестов пакета НИСТ.

	Среднее значение, дисперсия (0.5,0.0833)		**Хи-квадрат (≤ 29.6)**	**Число неудачных последовательностей (≤ 19.4)**
T1	0.5029	0.0818	9.480	6
T2	0.5067	0.0812	11.040	5
T3	0.5028	0.0852	7.960	11
T4	0.4987	0.0818	14.200	5
T5	0.5001	0.0829	13.320	6

Псевдослучайные последовательности, сгенерированные НГПСЧ, успешно прошли все тесты на случайность.

Тестирование качества НГПСЧ

Тестирование НГПСЧ с помощью пакета тестов DIEHARD

Тесты DIEHARD — это набор из 15 статистических тестов для измерения качества последовательностей случайных чисел. Вместе они рассматриваются как один из наиболее строгих существующих наборов тестов.

С целью тестирования НГПСЧ с помощью пакета статистических тестов DIEHARD, была сгенерирована последовательность размером 11 МегаБайт

В результате применения пакета DIEHARD было сформировано 220 P-values и для того, чтобы интерпретировать эти эмпирические результаты, использованы два основных критерия: критерий Колмогорова-Смирнова (КС-тест) и критерий хи-квадрат.

Результаты тестирования качества НГПСЧ с помощью пакета тестов DIEHARD

Название теста	P-значение	Результат
1. Дни рождения	0.7416	успех
2. Пересекающиеся перестановки	0.9625	успех
	0.6870	
3. Ранги матриц (31x31 и 32x32)	0.6691	успех
	0.3837	
4. Ранги матриц (6x8)	0.3363	успех
5. Обезьяньи тесты на 20 бит-слов	0.6002	успех
6. Обезьяньи тесты (OPSO, OQSO, DNA)	0.6512	успех
	0.7687	
	0.6801	
7. Подсчёт единиц в потоке байтов	0.9258	успех
	0.5227	
8. Количество единиц в конкретных байтах	0.7666	успех
9. Тест на парковку	0.4150	успех
10. Тест на минимальное расстояние	0.7721	успех
11. Тест случайных сфер	0.8041	успех
12. Тест сжатия	0.6126	успех
13. Тест пересекающихся сумм	0.5029	успех
14. Тест последовательностей (восходящие и нисходящие)	0.5434	успех
	0.5101	
15. Тест игры в кости (подсчитываются победы, количество бросков в каждой игре)	0.7490	успех
	0.3700	

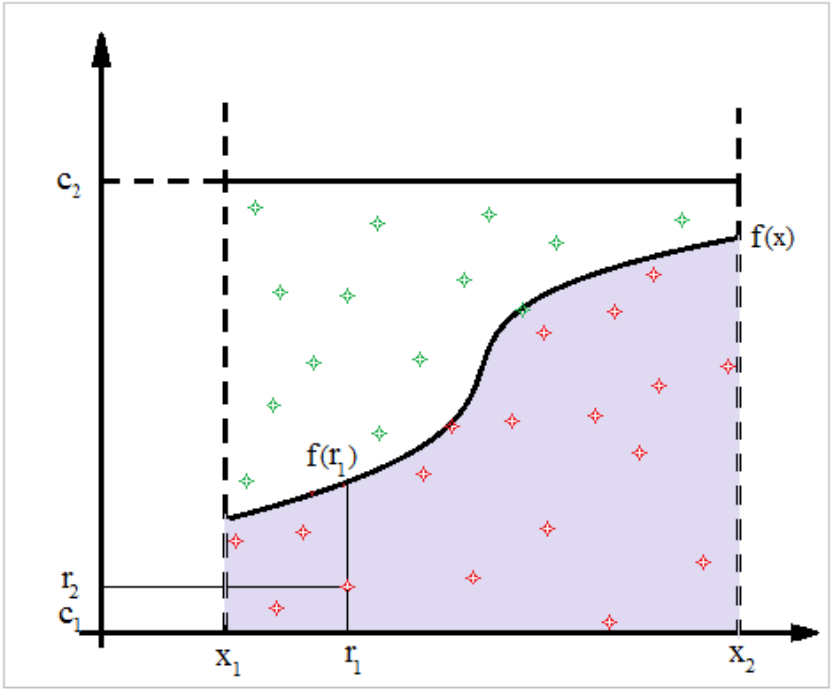
Из таблицы видно, что последовательность, сгенерированная с помощью НГПСЧ, успешно прошла все тесты пакета DIEHARD.

Использование метода Монте-Карло для оценки качества НГПСЧ

Метод статистического моделирования Монте-Карло использован для тестирования качества предложенного генератора путем вычисления интеграла.

Принцип метода Монте-Карло

$$\frac{N_2}{N_1} \cong \frac{\int_{x_1}^{x_2} f(x)dx}{(x_2 - x_1)(c_2 - c_1)}$$



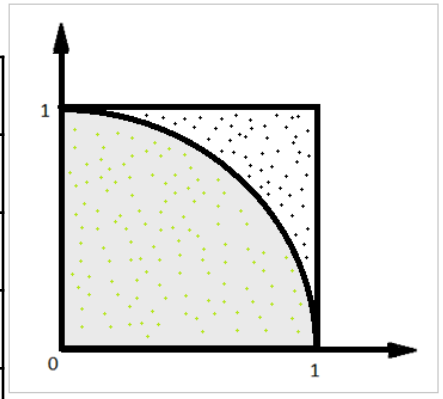
Количество точек, попавших под кривую (N_2), по отношению к общему числу точек (N_1), пропорционально площади под кривой (величине интеграла) по отношению к площади испытуемого прямоугольника.

Использование метода Монте-Карло для оценки качества НГПСЧ

С помощью метода Монте-Карло выполнено 4 эксперимента:

Первый эксперимент

Вычисление математической константы π с помощью двух генераторов: НГПСЧ и функции (Randi) Матлаба.



Number of random points	НГПСЧ		Matlab's RNG	
	estimated value	| π-est(π)|	estimated value	| π-est(π)|
100	3.1200	0.0216	3.4000	0.2584
1000	3.1160	0.0256	3.1000	0.0416
10000	3.1400	0.0016	3.1448	0.0032
100000	3.1422	0.0007	3.1433	0.0017
1000000	3.1414	0.0002	3.1413	0.0003

Полученные результаты показали, что НГПСЧ работает лучше функции Rand.

Использование метода Монте-Карло для оценки качества НГПСЧ

Второй эксперимент

Вычисление математического интеграла двухмерной функции с помощью двух генераторов - построенного НГПСЧ и функции (Randi) Матлаба.

$$f(x,y) = \sqrt{1 + x^3 + y^2 + x \cdot y} - 1,\ (x,y) \in [0,1]^2 \qquad \frac{N_2}{N_1} \cong 0.3360$$

Number of random points	НГПСЧ		Matlab's RNG	
	estimated value	| I-est(I)|	estimated value	| I-est(I)|
100	0.3400	0.0040	0.3600	0.0240
1000	0.3340	0.0020	0.3390	0.0030
10000	0.3384	0.0024	0.3389	0.0029
100000	0.3355	0.0005	0.3336	0.0024
1000000	0.3365	0.0005	0.3370	0.0010

Полученные результаты показали, что НГПСЧ работает лучше функции Randi.

Использование метода Монте-Карло для оценки качества НГПСЧ

Третий эксперимент

Вычисление математического интеграла трёхмерной функции с помощью двух генераторов - построенного НГПСЧ и функции (Randi) Матлаба.

$$f(x,y,z) = \sqrt{1 + x^4 + y^2 + x \cdot y \cdot z - z^2 + y \cdot z} - 1,$$
$$(x,y,z) \in [0,1]^3$$

$$\frac{N_2}{N_1} \cong 0.2277$$

Number of random points	НГПСЧ		Matlab's RNG	
	estimated value	| I-est(I)|	estimated value	| I-est(I)|
100	0.2800	0.0523	0.3100	0.0823
1000	0.2620	0.0343	0.2600	0.0323
10000	0.2310	0.0033	0.2422	0.0145
100000	0.2246	0.0269	0.2224	0.0053
1000000	0.2253	0.0266	0.2236	0.0041

Полученные результаты показали, что НГПСЧ часто работает лучше функции Randi.

Использование метода Монте-Карло для оценки качества НГПСЧ

Четвёртый эксперимент

Вычисление математического интеграла четырёхмерной функции с помощью двух генераторов - построенного НГПСЧ и функции (Randi) Матлаба.

$$f(x,y,z,u)=\sqrt{5+x^4+y^2+u^3+x\cdot y\cdot z-u\cdot z^2+y\cdot z}-2\,,\qquad \frac{N_2}{N_1}\cong 0.4441$$
$$(x,y,z,u)\in[0,1]^4$$

Number of random points	НГПСЧ		Matlab's RNG	
	estimated value	| I-est(I)|	estimated value	| I-est(I)|
100	0.4800	0.0359	0.5200	0.0759
1000	0.4650	0.0209	0.4690	0.0249
10000	0.4490	0.0049	0.4385	0.0056
100000	0.4447	0.0006	0.4434	0.0007
1000000	0.4445	0.0004	0.4435	0.0006

Полученные результаты показали, что НГПСЧ работает лучше функции Randi.

Использование метода Монте-Карло для оценки качества НГПСЧ

Заключение

Таким образом, на основании экспериментов можно заключить, что предложный генератор НГПСЧ действительно лучше псевдослучайного генератора среды Матлаба (R2012a version 7.14.0.739).

Полученные результаты показали, что НГПСЧ удовлетворяет всем требованиям к качественным генераторам псевдослучайных чисел.

Сравнение НГПСЧ с другими генераторами псевдослучайных чисел

НГПСЧ был сравнен с 21 известным генератором:

- 16 генераторов, включенных в пакет DIEHARD;
- 5 генераторов псевдослучайных чисел включенных в несколько высокоуровневых языков программирования (Ява, Дельфи, Visual Basic, Matlab, среда Wolfram Mathematica).

Сравнение было выполнено с помощью тестов пакета НИСТ.

Сравнение НГПСЧ с другими генераторами псевдослучайных чисел

Название генератора	хи-квадрат (≤ 29.6)	Число неуданых последовательностей (< 19*5)
НГПСЧ	+	+ (33)
1- Multiply with carry (MWC)	+	+ (47)
2- MWC on pairs of 16bits	+	- (51)
3- the mother of all RNGs	-	+ (55)
4- Kiss RNG	-	+ (54)
5- Combo RNG	+	+ (55)
6- The lagged Fibonacci-MWC combination ULTRA	-	+ (44)
7- A combination of MWC & subtract with borrow (SWB)	-	+ (50)
8- Extended conqruential	-	+ (43)
9-The super Duper generator RNG	+	+ (63)
10- Substract with borrow	-	+ (46)
11- Any specified congruential	-	+ (52)
12- The 31-bit ran2 from Numerical Recipes	-	+ (51)
13- Any specified shift register generator 31 or 32 bits	-	+ (53)
14- The system generator in Microsoft Fortran	-	+ (58)
15- Any lagged-Fibonacci	+	- (94)
16- An inverse conqruential	-	+ (45)
сравнения НГПСЧ с генераторами в языках программирования высокого уровня		
17- Java NB 8.1(Random.nextDouble())	-	+(47)
18- delphi Embarcadero RAD Studio 10.1 Berlin (Random)	-	+(45)
19- VB .Net Visual Studio 2013 (Random.next())	-	+(51)
20- Wolfarm Mathematica 7.0.0 (RandomReal[])	-	+(61)
21- MatLab R2012a (7.14.0.739) (Rand)	+	+(51)

Выводы

В заключение можно сказать, что НГПСЧ имеет большой период, хорошие статистические свойства, высокое быстродействие и эффективность, высокую диффузионную ёмкость, низкое энергопотребление, устойчивую иммунность против алгебраических атак.

НГПСЧ генерирует псевдослучайные последовательности неотличимые от истинно случайных. Они могут быть безопасно использованы для практического решения многих задач во многих предметных областях (телекоммуникации, криптография, моделирование и т.д.).

Список опубликованных работ

ВАК

1. Аникин И.В., Альнаджар Х.Х. Генератор псевдослучайных чисел, построенный на нечеткой логике // Информация и безопасность – 2015. - Том 18, № 3. - С. 376-379.
2. Аникин И.В., Альнаджар Х.Х. Анализ стойкости генератора псевдослучайных чисел, основанного на нечеткой логике, к корреляционным атакам// Информация и безопасность – 2016. - Том 19, № 3. - С. 413-416.
3. Аникин И.В., Альнаджар Х.Х. “Исследование параметров генератора псевдослучайных чисел, основанного на нечеткой логике”//Вестник технологического университета- 2016.- Том 19, № 12.- С. 124-127.
4. Аникин И.В., Альнаджар Х.Х. “Выбор примитивных полиномов для генератора псевдослучайных чисел, основанного на нечеткой логике”//Вестник КГЭУ- 2016.- Том 19, № 2(30).- С. 38-51.

SCOPUS

5. I.V. Anikin, K. Alnajjar, “Fuzzy stream cipher system,”, Proceedings of 2015 International Siberian Conference on Control and Communications, SIBCON 2015, Omsk, 2015.
6. I.V. Anikin, K. Alnajjar, “Pseudo-Random Number Generator Based on Fuzzy Logic”, Proceedings of 2016 International Siberian Conference on Control and Communications, SIBCON 2016, Moscow, 2016.

Спасибо за внимание!