Автоматная модель представления нелинейных максимальных псевдослучайных последовательностей над конечным полем

В.М. Захаров, С.В. Шалагин, Б.Ф. Эминов

Семинар «Методы моделирования», 17.03.17

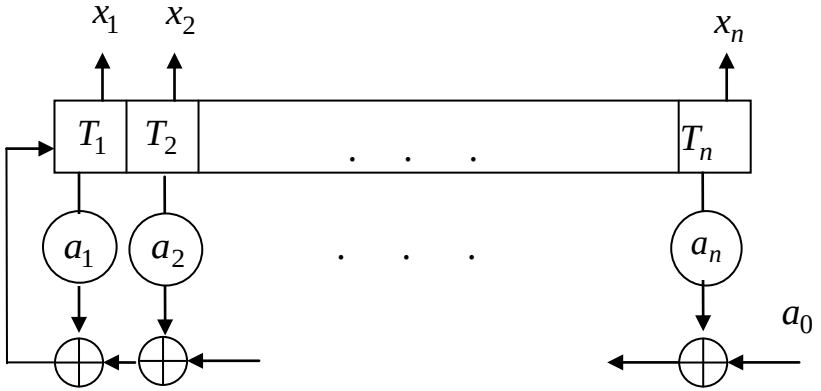
Введение

Известные псевдослучайные генераторы

1. $\boldsymbol{x_{i+1} \equiv g(x_i) \bmod p}$, $x_i \in \overline{1, p-1}$, период $L \leq p$-1

2. Генератор $x_{i+1} = a^{x_i} \bmod p$, $x_i \in \overline{1, p-1}$, период $L < p$-1

3. Автономный линейный автомат $\boldsymbol{X_{i+1}=AX_i}$, $x_i \in \overline{1,2^n-1}$, период $L = 2^n - 1$



Генератор M-последовательности

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$

4. **Генератор** нелинейной псевдослучайной последовательности **де-Брейна**

$$f_0 = F(x) \oplus \overline{(x_1 \cdot \ldots \cdot x_{n-1})},\ f_0 \in \overline{0,2^n - 1},\ \text{период } L = 2^n$$

Последовательности де-Брейна (основанные на f_0):

- имеют максимальное значение критерия «*линейная сложность*», равное $2^n - 1$,
- сбалансированы по количеству нулей и единиц на периоде $L = 2^n$.

Направление: применение к элементам *M*-последовательности дополнительного преобразования:

- в виде некоторой внешней логики (нелинейной функции усложнения (**НФУ**))
- для усложнения ее аналитического строения.

Подход: $y_j \equiv (Q^j) \bmod p$

нелинейное преобразование - Алгоритм возведения в степень по модулю простого числа:

- алгоритм вычисления дискретного логарифма,
- если Q - первообразный корень (примитивный элемент) по модулю p.

Свойства:

1) $j, y_j \in M_1 = \{1, 2, \ldots, p\text{-}1\}$, $\boldsymbol{F_1: M_1 \rightarrow M_1}$ **- инъекция**

2) $(\boldsymbol{Q^{p-1}})\mathbf{mod}\ \boldsymbol{p} \equiv \mathbf{1},\ 1 < Q < p-1.$

3) **нелинейность - не** выполняется **условие линейности** преобразования над конечным полем:

$$\boldsymbol{j = j_1 + j_2}\ , \qquad \mathbf{g}(\boldsymbol{j}_1 + \boldsymbol{j}_2)(\mathbf{mod}\ \boldsymbol{p}) \equiv [\mathbf{g}\ (\boldsymbol{j}_1) + \boldsymbol{g}(\boldsymbol{j}_2)]\ \mathbf{mod}\ \boldsymbol{p}$$

Цель работы: исследовать возможности построения математической **модели генератора** ПСП периода $\boldsymbol{L=2^n}$, $\boldsymbol{n > 1}$, с **нелинейной функцией усложнения**, основанной на **Алгоритме.**

1. Постановка задачи

Рассмотрим генератор ПСП в виде конечного автономного автомата с функцией выхода:

$$\mathbf{КА = (}S, Y, \delta, \lambda, s_0\mathbf{)}, \qquad (1)$$

S; Y ; $\delta: S \to S$ - функция переходов;

$\lambda: S \to Y$ - функция выхода.

Примем: состояния автомата (1) - вектора $X = (x_1, x_2, ..., x_n)$;

- выходные буквы - вектора $Z = (z_1, z_2, ..., z_n)$.

Ограничения:

Функция переходов реализуется как:

- генератор последовательности де-Брейна с периодом 2^n
- на основе РС с нелинейной функцией обратной связи вида:

$$f_0 = F(x) \oplus \overline{(x_1 \cdot \ldots \cdot x_{n-1})}.$$

Функция выхода λ выполняет **однозначное** отображение

$$\boldsymbol{Z = \Phi(X): G(2)^n \rightarrow G(2)^n,} \qquad (2)$$

где $G(2)^n$ – множество n-мерных двоичных векторов, $|G(2)^n| = 2^n$.

Рассмотрим нелинейное преобразование - **Алгоритм**

$$y_j \equiv (Q_h^j) \bmod p, \qquad (3)$$

где p - простое число, j - целое число,

- Q_h – заданный первообразный корень (примитивный элемент) по модулю p,

- $h = 1, 2, \ldots, \varphi(p-1)$ (число первообразных корней при заданном модуле p равно значению функции Эйлера $\varphi(p-1)$),

- Q_h принимает значения из интервала $1 < Q_h < p-1$.

Отметим следующие свойства С1 и С2 **Алгоритма.**

Введем множество $\boldsymbol{M_1 = \{1, 2, \ldots, p\text{-}1\}}$.

Свойство С1. **Алгоритм** выполняет инъективное отображение
$\boldsymbol{F_1: M_1 \rightarrow M_1}$. Отображение F_1 есть перестановка, заданная на M_1.

Свойство С2. При реализации **Алгоритмом** отображения $\boldsymbol{F_1: M_1 \rightarrow M_1}$ выполняется соответствие вида

$$\boldsymbol{j = (p-1)/2 \rightarrow y_j = p-1} \qquad (4)$$

Решаемая задача - построение для автоматной модели (1) **нелинейной функции** выхода, реализующей инъективное отображение (2), где n - четное, $n > 1$, на основе **Алгоритма**.

2. Анализ задачи, подход к решению

Из свойств С1, С2 следует, что для реализации инъективного отображения (2):

$$Z = \varphi(X): G(2)^n \rightarrow G(2)^n, |G(2)^n| = 2^n$$

для **Алгоритма** необходимым условием является выполнение соотношения:

модуль $\boldsymbol{p > 2^n, n > 1}$.

Отметим: чем больше величина $\Delta = \boldsymbol{p - 2^n}$, тем больше отличается множество Y по составу и величине элементов от множества S.

Имеется **два множества** простых чисел, при которых величина Δ имеет **минимальное** значение **Δ=1**:

1. Простые числа Мерсенна – числа вида $M(p)=2^n-1$, $n = p_i$, $i=1,2,\ldots,47$, $p_{47} = 43112609$.

2. Простые числа Ферма - числа вида $p = 2^m + 1$, где $m=1, 2, 4, 8, 16$:

$p_0=2^1+1=3$ $p_1=2^2+1=5,$ $p_2=2^4+1=17,$

$p_3=2^8+1=257,$ $p_4=2^{16}+1=65537.$

Обозначим множество $\{p_1, p_2, p_3, p_4\}$ простых чисел Ферма символом M_F.

Рассмотрим решение задачи реализации инъективного отображения вида (2) на основе **Алгоритма**

- с применением модуля $p \in M_F$

- для случая $n=m$ = 2, 4, 8, 16.

Введем множество $M_3 = \{0, 1, 2, \ldots, 2^m-1\}$, $|M_3|=2^m$, m=2, 4, 8, 16.

Построим инъективное отображение

$$F_2: M_3 \rightarrow M_3$$

Отметим следующее свойство **Алгоритма**, которое представим как

Утверждение 1. Пусть в **Алгоритме** выполняются следующие условия:

- модуль $p \in M_F$,
- $1 < Q_h < p-1$,
- величина $2^m = p-1$, $m = 2, 4, 8, 16$.

Тогда **Алгоритм** выполняет инъективное отображение вида

$$\boldsymbol{F_3}: M_3 = \{0, 1, 2, \ldots, 2^m-1\} \rightarrow M_4 = \{1, 2, \ldots, 2^m\text{-}1, 2^m\},$$

где представлено соответствие

$$\left(j = \left(2^m\right)/2\right) \rightarrow \left(y_j = 2^m\right). \qquad (5)$$

Справедливость утверждения 1 следует из свойств С1, С2.

Обозначим символом $A_м$ алгоритм, являющийся следующей модификацией **Алгоритма**. В качестве алгоритма $A_м$ будем рассматривать алгоритм, который отличается от **Алгоритма** только тем, что

- при $p \in M_F$, $j = 2^m/2$ и $1 < Q_h < p-1$
- выполняет вместо преобразования (5) преобразование вида:

$$\left(j = \left(2^m\right)/2 \rightarrow y_j = 0\right).$$

Следствие 1 (из утверждения 1). Пусть в **Алгоритме**

- переменная j принимает значения из множества M_3,
- модуль $p \in M_F$,
- $2^m = p-1$, $m = 2, 4, 8, 16$ и
- $1 < Q_h < p-1$.

Тогда инъективное отображение

$$\boldsymbol{F_2: M_3 \rightarrow M_3 = \{0, 1, 2, \ldots, 2^m - 1\}}$$

можно выполнить алгоритмом $\boldsymbol{A_м}$.

Из следствия 1 **вытекает**:

1) применение в автоматной модели (1) алгоритма $\boldsymbol{A_м}$ для реализации функции выхода позволяет выполнять инъективное отображение (2), где $n = m = 2, 4, 8, 16$;

2) получаемая ПСП на выходе НФУ, реализованной по алгоритму $\boldsymbol{A_м}$, имеет абсолютно **максимальный период** $L = 2^n$, где $n = m = 2, 4, 8, 16$;

3) по структуре выходная ПСП является перестановкой элементов последовательности де-Брейна.

Однако величина **периода** получаемых ПСП на выходе автоматной модели (1) **ограничена** величиной **модуля** $p \in M_F$.

Предлагается решение задачи - реализация инъективного отображения (2) при $\boldsymbol{n > m}$ на основе алгоритма $\boldsymbol{A_м}$.

3. Модель функции усложнения

Примем $\boldsymbol{n \geq m}$.

Выполним **разбиение**

n-мерного **двоичного вектора** $\boldsymbol{X}$,

$n \bmod m \equiv 0$,

на $\boldsymbol{k}$ блоков –

m–разрядные двоичные векторы X_i, $i = \overline{1,k}$,

где $\boldsymbol{k = n/m}$, $m = 2, 4, 8, 16$.

Подобное разбиение проведем и для вектора $Z = (Z_i)$, $i = \overline{1,k}$.

Двоичные вектора X_i и Z_i , $i = \overline{1,k}$, принимают значения из множества $\mathbf{M_3=\{0,1,2, \ldots, 2^m-1\}}$.

Введем в рассмотрение систему элементов вида

$$(\beta_1, \beta_2, \ldots, \beta_k) \qquad (6)$$

где β_i, $i = \overline{1,k}$ - однозначное преобразование (инъекция), выполняемое алгоритмом $A_м$ при m = 2, 4, 8, 16, двоичных значений вектора X_i, $i = \overline{1,k}$, **по модулю** $p \in M_F$ при заданном Q_h, $1 < Q_h < p-1$, в двоичные значения вектора Z_i.

Примем $n = h \cdot m$, $k = h$, m = 2, 4, 8, 16, $h = \overline{1, \varphi(p-1)}$.

Требуется доказать, что НФУ в модели (1), представляемая как система (6), **при ограничениях**

1) β_i – инъекция,

2) $1 < Q_h < p-1$,

3) $n = k \cdot m$, $k = h$

выполняет инъективное отображение (2):

$$Z = \varphi(X): \mathrm{G}(2)^n \rightarrow \mathrm{G}(2)^n$$

Утверждение 2 (основное). Если в модели (1) нелинейная функция усложнения определена как система (6), то модель (1) выполняет инъективное отображение (2).

Справедливость утверждения 2 следует из свойств образов и прообразов для инъективного отображения.

Систему преобразований (6) будем рассматривать как модель функции усложнения для реализации инъективного отображения (2) в автомате (1).

Применение в преобразованиях β_i, $i=\overline{1,k}$, системы (6), при фиксированном модуле $p \in M_F$, различных примитивных элементов Q_h позволяет

параметрически (меняя Q_h) менять структуру ПСП на выходе НФУ путем перестановки элементов последовательности де-Брейна.

Замечание 1. Число первообразных корней для применения их в алгоритме $\mathbf{A_м}$ при модуле $p \in M_F$ равно:

- для $p_1 = 5$: $h(p_1)=2$;
- для $p_2 = 17$: $h(p_2)=8$;
- для $p_3 = 257$: $h(p_3)=128$;
- для $p_4 = 65537$: $h(p_4)= 32768$.

Из **утверждения** 2 **следует** возможность:

- реализации определенных модификаций системы (6);
- получения на основе автоматной модели (1) различных по размеру ансамблей нелинейных ПСП.

4. **Оценка ансамбля выходных нелинейных ПСП**

Параллельная реализация системы (6)

Пусть $\boldsymbol{n = k \cdot m}$, m = 2, 4, 8, 16, $n \bmod m \equiv 0$, k определяется из условия

$$\boldsymbol{k = h(p_i)},\ i = 1, 2, 3, 4.$$

В этом случае на **выходе автомата** (1)

- при фиксированной функции переходов и
- с примитивным полиномом степени $n = m \cdot h(p_i)$,

можно **получить**:

ансамбль $\boldsymbol{V_h = h(p_i)!}$ нелинейных псевдослучайных последовательностей с заданным периодом $L = 2^n$,

где $\boldsymbol{n = m \cdot h(p_i)}$, i =1, 2, 3, 4.

Пример. Пусть для модели (1) в системе (6):

- в элементах β_i применяется модуль $p_3 = 257$ и $k = h = 128$,
- и в генераторе де-Брейна применяется примитивный полином степени $n = m \cdot h(p_i) = 1024$, $m = 8$.

Тогда:

- период ПСП на выходе автомата (1) равен $L = 2^{1024}$ и
- ансамбль $V_h = 128!$

Замечание 2. Нижняя оценка величины $V_h = h(p_4)$!

при $\boldsymbol{n = m \cdot 32768}$ и

периоде $\boldsymbol{L = 2^{m \cdot 32768}}$,

где $m = 16$

определяется значением

$$\boldsymbol{V_h = O(2^{32768})}.$$

Последовательная реализация системы (6)

Примем

$\boldsymbol{n \geq h \cdot m,}$

$m = 2, 4, 8, 16,$

$n \bmod m \equiv 0,$

$h = \overline{1, \varphi(p-1)}$ и $\boldsymbol{k \geq h}$ (данные условия определяют возможность кратного применения в системе (6) элемента β_i , $i = \overline{1, k}$).

Преобразование *n*-разрядного **вектора *X***

в ***n*-**разрядный вектор Z

выполняется одним элементом β последовательно

m - разрядными блоками за ***k*** раундов.

В раундах, на периоде 2^n, преобразование в элементе β выполняется с чередованием элементов Q_h (хранимыми в отдельной памяти).

Замечание 3. Для последовательной схемы размер V ансамбля формируемых нелинейных последовательностей

периода $L = 2^n$,

$n \bmod m = 0$,

$m = 2, 4, 8, 16$,

находится в пределах

$$2^{n/2} \le V \le 2^{15n/16}$$

Заключение

1.Предложена **автоматная модель** формирования **нелинейных** псевдослучайных **последовательностей** с заданным периодом $L = 2^n$, где $n>1$, $n \equiv 0 \bmod m$, m=2,4,8,16 с функцией выхода, реализованной на основе системы нелинейных модулярных операций по модулю, принадлежащему к множеству простых чисел Ферма.

2. Определены и аналитически **обоснованы алгоритмические свойства** автоматной модели (утверждение1, следствие 1, утверждение 2).

3. На основе **алгоритмических** свойств нелинейная **функция выхода** автомата

- представлена как **инъективная функция** аналитического **усложнения**
  - псевдослучайная перестановка элементов последовательности де- Брейна.

4. **Изменение структуры** выходных **ПСП** на периоде $L = 2^n$ можно получить

псевдослучайной **перестановкой** значений первообразных **корней** по модулю числа Ферма.

5. **Размер ансамбля** выходных нелинейных **ПСП** оценивается величиной

$$\boldsymbol{O(2^n)},\ n \equiv 0 \bmod m,\ m=2,4,8,16.$$

Литература

1. Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР, 1980, т. 68, №5. С.59-90.

2.Schneier B. Applied cryptography, 2nd Edition, John Wiley & Sons (1996). [Перевод: Шнайер Б. Прикладная криптография. http://www.ssl.stu.neva.ru/ psw/crypto.html]

3. Алферов А.П. и др. Основы криптографии: учеб. пособие для вузов. М.: Гелиос АРВ, 2002. 480 с.

4. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.:КУДИЦ-ОБРАЗ, 2001. 368 с.

5. Стельмашенко Б.Г., Тараненко П.Г. Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации. Зарубежная радиоэлектроника, №12, 1988. С.3-16.

6. Столов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности // Kazan Federal University [Электронный ресурс]. 1995-2016. http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf

7. Захаров В.М., Шалагин С.В. Реализация генератора нелинейных псевдослучайных последовательностей с функцией усложнения на основе чисел Ферма // Сб. статей XIII Межд.научно-техн.конф. «Новые информационные технологии и системы» (НИТиС-2016). Пенза, 2016. С. 81-83.

8. Захаров В.М., Зелинский Р.В., Шалагин С.В. Модель функции усложнения над полем GF(2) в генераторе псевдослучайных последовательностей // Прикладная дискретная математика. Приложение. 2014, № 7. С. 67-68.

9.Захаров В.М. Шалагин С.В. Математическая модель генератора псевдослучайных последовательностей на основе нелинейных функций обратной связи//Вестник технологического университета. Т.19, №21, 2016. С.131-138.

10. Бухштаб А.А. Теория чисел. М.: Просвещение, 1966. 384 с.

11. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие. Казань: Казан. гос. ун.-т, 2011. 192 с.

12. Самсонов Б.Б, Плохов Е.М., Филоненков А.И. Компьютерная математика. Ростов-на-Дону: Феникс, 2002. 512 с.

Приложение

Отметим: операцию возведения в степень по модулю $p \in M_F$ по **Алгоритму** можно реализовать путем применения известной вычислительной процедуры

Пример 1. Реализация **Алгоритма**.

Пусть $m = 4$, $p_2 = 17$, $Q_h = 3$.

1) Зададим текущее двоичное значение j.

Пусть $j = (x_0\, x_1\, x_2\, x_3)_2 = 1011_2$.

2) Заполним следующую таблицу

j	x_0	x_1	x_2	x_3
Q_h	$б_0$	$б_1$	$б_2$	$б_3$

где $б_0 = Q_h = 3$- заданный примитивный элемент по модулю p=17,

$$б_{l+1} = \begin{cases} б_l^2 \bmod p, \text{если } x_{l+1} = 0 \\ б_l^2 \cdot б_0 \bmod p, \text{если } x_{l+1} = 1 \end{cases}, \; l = 0, 1, 2, 3.$$

3) Результат $y_j = б_3$ (двоичный 4-х разрядный код) считывается из последней ячейки второй строки. Для j = 1011 получаем $y_j = б_3$=0111.

Пример 2. Пусть в автомате (1) функция перехода δ реализует

- на основе примитивного полинома $f(x) = x^4 + x + 1$
- с периодом L=16
- последовательность де-Брейна (последовательность 4-разрядных векторов X).

В этом случае вектор X в (1) принимает следующие 16 различных 4-разрядных двоичных значений
X = (0001, 0000, 1000, 0100, 0010, 1001, 1100, 0110, 1011, 0101, 1010, 1101, 1110, 1111, 0111, 0011).

Примем - система (6) представлена парой преобразований (β_1, β_2), где:

- $m = 2$,
- элемент β_1 выполняет:

преобразование вида $y_j \equiv (3^j) \bmod 5$

с $Q_1 = 3$

над каждой первой парой бит значения вектора X

- и элемент β_2 выполняет:

преобразование вида $y_j \equiv (2^j) \bmod 5$

с $Q_2 = 2$

над каждой второй парой бит значения вектора X.

Тогда на выходе НФУ можно получить следующую последовательность с периодом L=16.

Z =(0110, 0101, 0001, 1101, 0100, 0010, 1001, 1100, 0011, 1110, 0000, 1010, 1000, 1011, 1111, 0111).