Автоматная модель представления нелинейных псевдослучайных последовательностей с функцией выхода на основе системы инъективных преобразований

**Человек:** Предметом исследования являются методы усложнения аналитического строения псевдослучайных последовательностей путем применении к элементам заданной исходной псевдослучайной последовательности дополнительного преобразования в виде нелинейной внешней логики - нелинейной функции усложнения. Целью работы является определение и алгоритмическое построение математической модели нелинейной функции усложнения, представляемой на основе модулярной операции возведения в степень по простому модулю, позволяющей получать нелинейные псевдослучайные последовательности, обладающие на заданном максимальном периоде статистическими свойствами, приближающимися к свойствам случайной равновероятной последовательности. Для представления модели используется формализм теории автоматов, теорий конечного поля, модулярной арифметики и простых чисел. Предложена автоматная модель формирования нелинейных псевдослучайных последовательностей с заданными периодами L = 2^n-1 и L = 2^n, n >1, отличающаяся функцией выхода, представленной в виде нелинейной функции усложнения на основе системы нелинейных преобразований по модулям, принадлежащих к множеству простых чисел Ферма. Доказано, что функция выхода автомата, представляется как инъективная функция, выполняющая на основе нелинейных модулярных операций на периоде L = 2^n перестановку элементов последовательности де-Брейна. Показано, что алгоритмическая модель функции выхода автомата позволяет менять структуру нелинейных последовательностей путем перестановки по псевдослучайному закону значений первообразных корней по модулю числа Ферма. Размер ансамбля нелинейных последовательностей, формируемых нелинейной функцией усложнения, зависит от числа первообразных корней и определяется нижней оценкой вида О(2^n), n>1.

**Key words:** псевдослучайная последовательность, автоматная модель, функция усложнения, инъективное преобразование, последовательность де-Брейна, М-последовательность, простые числа Ферма, нелинейная модулярная операция, первообразные корни, ансамбль последовательностей

=================================

**FastText\_KMeans\_Clean:** 1.Постановка задачи. Следствие 1 (из утверждения 1). - для р 1 = 5: H (p 1)= (5-1)=2;. Утверждение 2 (основное). n =k· m > H(pa )·m , , m = 2, 4, 8, 16. Пусть в (1) задан период L =2n последовательности де-Брейна, например, n = 128, m = 2, модуль р 1 = 5 и заданы элементы Q 1 = 2 и Q 2 = 3, вектор Х разбит на k = n/m двухразрядных блоков (Хi, ). Данную модификацию конечно-автоматной модели (1) обозначим символом КАY . 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна.

**Key words part:** 0.7

=================================

**FastText\_KMeans\_Raw/:** 1.Постановка задачи. Из свойств С1-С3 следует:. 2) Заполним следующую таблицу. Пусть j в (4) принимает значения из множества М 3, модуль рМ F , 2m = p−1, m = 2, 4, 8, 16 и 1 < Qh < p –1. 3. Модель функции усложнения. Следствие 2 (из утверждения 2). Если нелинейная функция усложнения определена как система (9) с ограничением (12), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y. Замечание 2.При реализации в КАY системой (9) отображения при ограничениях (10) и (12) получаемое множество Y отличается от множества S двумя n -разрядными векторами: Y включает нулевой вектор Z – вектор Z 0, все n разрядов которого содержат значение 0 и не содержит вектор Z =(Z i ), где у m - разрядного вектора Z i , , m =2, 4, 8, 16, младший разряд содержит значение 1. 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна.

**Key words part:** 0.7333333333333333

=================================

**FastText\_PageRank\_Clean/:** 1.Постановка задачи. (S , Y , , , s 0), (1). Пусть j =(х 0 х 1 х 2 х 3)2= 1011. Из следствия 1 вытекает следующее:. Утверждение 2 (основное). 5. Автоматная модель формирования. Следствие 3 (из утверждения 2). Следствие 4 (из утверждения 2).

**Key words part:** 0.36666666666666653

=================================

**FastText\_PageRank\_Raw/:** 1.Постановка задачи. Z = (X): G(2)n → G(2)n, (3). Из свойств С1-С3 следует:. 2) Заполним следующую таблицу. Следствие 1 (из утверждения 1). Следствие 2 (из утверждения 2). Следствие 3 (из утверждения 2). Следствие 4 (из утверждения 2).

**Key words part:** 0.3

=================================

**Mixed\_ML\_TR/:** Следствие 1 (из утверждения 1). Пусть j в (4) принимает значения из множества М 3, модуль рМ F , 2m = p−1, m = 2, 4, 8, 16 и 1 < Qh < p –1. (β1, β2, …, βk) (9). где βi, - однозначное преобразование (инъекция), выполняемое алгоритмом Ам при m = 2, 4, 8, 16 двоичных значений вектора Хi, , по модулю рМ F при заданном Qh , 1 < Qh < p –1, в двоичные значения вектора Zi . Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m . Если нелинейная функция усложнения определена как система (9) с ограничением (12), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y. Замечание 2.При реализации в КАY системой (9) отображения при ограничениях (10) и (12) получаемое множество Y отличается от множества S двумя n -разрядными векторами: Y включает нулевой вектор Z – вектор Z 0, все n разрядов которого содержат значение 0 и не содержит вектор Z =(Z i ), где у m - разрядного вектора Z i , , m =2, 4, 8, 16, младший разряд содержит значение 1. 1. Представленная автоматная модель формирования нелинейных псевдослучайных последовательностей с заданными периодами L = 2n и L = 2n −1, где n> 1, n ≡ 0 mod m , m =2,4,8,16, отличается видом модели функции выхода, задаваемой системой, реализующей k = n /m нелинейных операций возведения в степень по модулю, принадлежащему к множеству простых чисел Ферма и выполняющей инъективное преобразование. 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна. 3. Определены и аналитически обоснованы алгоритмические свойства автоматной модели (следствие 3, следствие 4), определяющие аналитическое усложнение ПСП на периоде L = 2n −1: функция выхода автомата порождает на основе нелинейных модулярных операций нелинейную ПСП, квазиподобную М -последовательности по статистическим (частотным) свойствам на периоде 2n −1.

**Key words part:** 0.8666666666666667

=================================

**MultiLingual\_KMeans/:** Следствие 1 (из утверждения 1). Пусть j в (4) принимает значения из множества М 3, модуль рМ F , 2m = p−1, m = 2, 4, 8, 16 и 1 < Qh < p –1. (β1, β2, …, βk) (9). где βi, - однозначное преобразование (инъекция), выполняемое алгоритмом Ам при m = 2, 4, 8, 16 двоичных значений вектора Хi, , по модулю рМ F при заданном Qh , 1 < Qh < p –1, в двоичные значения вектора Zi . 3. Определены и аналитически обоснованы алгоритмические свойства автоматной модели (следствие 3, следствие 4), определяющие аналитическое усложнение ПСП на периоде L = 2n −1: функция выхода автомата порождает на основе нелинейных модулярных операций нелинейную ПСП, квазиподобную М -последовательности по статистическим (частотным) свойствам на периоде 2n −1.

**Key words part:** 0.5666666666666667

=================================

**Multilingual\_PageRank/:** Примерами подобных работ, опубликованных в последние годы, являются [1–18]. - для р 1 = 5: H (p 1)= (5-1)=2;. 4. О величине ансамбля формируемых последовательностей. Примем, что в системе (9) ограничение имеет вид. Примем, что в системе (9) ограничение имеет вид. Пусть система (9) содержит только один элемент β, где модуль р 1 = 5. 5. Автоматная модель формирования. Вектор Z =(Z i ), , не содержится в Y вследствие того, что множество S не содержит вектор Х 0, которому алгоритм Ам ставит в соответствие данный вектор Z = (Z i ).

**Key words part:** 0.5

=================================

**RuBERT\_KMeans\_Without\_ST/:** Пусть j в (4) принимает значения из множества М 3, модуль рМ F , 2m = p−1, m = 2, 4, 8, 16 и 1 < Qh < p –1. Условия, принятые для системы (9): n = k · m ≥ H(pa )· m , , m = 2, 4, 8, 16 и утверждение 2 определяют разнообразие модификаций реализации системы (9) и получение на основе (1) различных по размеру ансамблей нелинейных ПСП. Следствие 2 (из утверждения 2). Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m . 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна.

**Key words part:** 0.7666666666666667

=================================

**RuBERT\_KMeans\_With\_ST/:** 1) применение в автоматной модели (1) алгоритма Ам для реализации функции выхода позволяет выполнять инъективное отображение (3), где n = m = 2, 4, 8, 16;. Применение в преобразованиях βi , , системы (9) при фиксированном модуле рМ F различных примитивных элементов Qh позволяет параметрически (меняя Qh ) менять структуру ПСП на выходе НФУ. Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m . Следствие 3 (из утверждения 2).

**Key words part:** 0.5

=================================

**RUBERT\_page\_rank\_Without\_ST/:** Примерами подобных работ, опубликованных в последние годы, являются [1–18]. 1.Постановка задачи. 3. Модель функции усложнения. 5. Автоматная модель формирования. Вектор Z 0 включен в Y в силу следствия 1.

**Key words part:** 0.43333333333333335

=================================

**RUBERT\_page\_rank\_With\_ST/:** 1.Постановка задачи. 2. Анализ задачи, подход к решению. Утверждение 2 (основное). 5. Автоматная модель формирования. : S → Y , |S |=|Y | =2n −1.

**Key words part:** 0.36666666666666653

=================================

**RUSBERT\_KMeans\_Without\_ST/:** Отметим следующие свойства алгоритма (4), вытекающие из свойств первообразных корней по модулю p [25]. Применение в алгоритме Ам при фиксированном модуле рМ F различных примитивных элементов Qh позволяет параметрически, меняя Qh в Ам (для каждого периода используется новый элемент Qh ), менять структуру ПСП на выходе алгоритма Ам и получать ансамбль формируемых ПСП, определяемый величиной H(pa ), , представленной в (8). Примем n = k · m ≥ H(pa )· m , , m = 2, 4, 8, 16 (данные условия определяют возможность кратного применения в (9) элемента βi , ). Следствие 2 (из утверждения 2). Следствие 2 обосновывает возможность при выполнении ограничения вида (10) в системе (9) получить на выходе автомата (1), при фиксированной функции переходов вида (2), с примитивным полиномом степени n = H(pa )·m , ансамбль Vh = H(pa )! нелинейных псевдослучайных последовательностей с заданным периодом L = 2n , где n = H(pa )·m , .

**Key words part:** 0.6

=================================

**RUSBERT\_KMeans\_With\_ST/:** F 2: М 3 → М 4 = {1, 2, …, 2m -1, 2m },. где представлено соответствие. Следствие 2 обосновывает возможность при выполнении ограничения вида (10) в системе (9) получить на выходе автомата (1), при фиксированной функции переходов вида (2), с примитивным полиномом степени n = H(pa )·m , ансамбль Vh = H(pa )! нелинейных псевдослучайных последовательностей с заданным периодом L = 2n , где n = H(pa )·m , . при m = 8, H 3 = 128, k 3 = n /8, = 128n /8=27n /8,. Если нелинейная функция усложнения определена как система (9) с ограничением (10), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y. Примем: в системе (9) ограничение имеет вид (12).

**Key words part:** 0.6333333333333333

=================================

**RUSBERT\_page\_rank\_Without\_ST/:** 1.Постановка задачи. Следствие 1 (из утверждения 1). Утверждение 2 (основное). Следствие 2 (из утверждения 2). Следствие 3 (из утверждения 2).

**Key words part:** 0.3

=================================

**RUSBERT\_page\_rank\_With\_ST/:** 1.Постановка задачи. Обозначим их символами С1, С2, С3. Следствие 2 (из утверждения 2). Следствие 3 (из утверждения 2). Следствие 4 (из утверждения 2).

**Key words part:** 0.3

=================================

**Simple\_PageRank/:** 2) получаемая нелинейная ПСП на выходе НФУ имеет абсолютно максимальный период L = 2n , где n = m = 2, 4, 8, 16 и по своей структуре является перестановкой элементов (векторов Х ) последовательности де-Брейна, формируемой по соотношению (2). Пусть в системе (9) при ограничении (10) в преобразованиях βi, , применяются различные элементы Qh , 1 < Qh < p –1, в соответствии с фиксированным модулем рМ F . Следствие 2 обосновывает возможность при выполнении ограничения вида (10) в системе (9) получить на выходе автомата (1), при фиксированной функции переходов вида (2), с примитивным полиномом степени n = H(pa )·m , ансамбль Vh = H(pa )! нелинейных псевдослучайных последовательностей с заданным периодом L = 2n , где n = H(pa )·m , . Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m . Если нелинейная функция усложнения определена как система (9) с ограничением (12), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y. Замечание 2.При реализации в КАY системой (9) отображения при ограничениях (10) и (12) получаемое множество Y отличается от множества S двумя n -разрядными векторами: Y включает нулевой вектор Z – вектор Z 0, все n разрядов которого содержат значение 0 и не содержит вектор Z =(Z i ), где у m - разрядного вектора Z i , , m =2, 4, 8, 16, младший разряд содержит значение 1. Пусть n = 4, р = 5, m = 2, k = 2 система (9) представлена парой преобразований (β1, β2), где β1 выполняется с Q 1=3 и β2 выполняется с Q 2 = 2 и функция переходов автомата КАY формирует последовательность векторов Х , принимающих следующие 15 различных четырехразрядных двоичных значений в соответствии с М-последовательностью, построенной на РС с s0 = 1000, по примитивному полиному f(x )=x 4+x +1: (1000, 0100, 0010, 1001, 1100, 0110, 1011, 0101, 1010, 1101, 1110, 1111, 0111, 0011, 0001).

**Key words part:** 0.7333333333333333

=================================

**TextRank/:** Следствие 2 обосновывает возможность при выполнении ограничения вида (10) в системе (9) получить на выходе автомата (1), при фиксированной функции переходов вида (2), с примитивным полиномом степени n = H(pa )·m , ансамбль Vh = H(pa )! нелинейных псевдослучайных последовательностей с заданным периодом L = 2n , где n = H(pa )·m , . Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m . Если нелинейная функция усложнения определена как система (9) с ограничением (12), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y. Замечание 2.При реализации в КАY системой (9) отображения при ограничениях (10) и (12) получаемое множество Y отличается от множества S двумя n -разрядными векторами: Y включает нулевой вектор Z – вектор Z 0, все n разрядов которого содержат значение 0 и не содержит вектор Z =(Z i ), где у m - разрядного вектора Z i , , m =2, 4, 8, 16, младший разряд содержит значение 1. Пусть n = 4, р = 5, m = 2, k = 2 система (9) представлена парой преобразований (β1, β2), где β1 выполняется с Q 1=3 и β2 выполняется с Q 2 = 2 и функция переходов автомата КАY формирует последовательность векторов Х , принимающих следующие 15 различных четырехразрядных двоичных значений в соответствии с М-последовательностью, построенной на РС с s0 = 1000, по примитивному полиному f(x )=x 4+x +1: (1000, 0100, 0010, 1001, 1100, 0110, 1011, 0101, 1010, 1101, 1110, 1111, 0111, 0011, 0001). 1. Представленная автоматная модель формирования нелинейных псевдослучайных последовательностей с заданными периодами L = 2n и L = 2n −1, где n> 1, n ≡ 0 mod m , m =2,4,8,16, отличается видом модели функции выхода, задаваемой системой, реализующей k = n /m нелинейных операций возведения в степень по модулю, принадлежащему к множеству простых чисел Ферма и выполняющей инъективное преобразование. 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна.

**Key words part:** 0.9333333333333332

=================================

**TF-IDF\_KMeans/:** (S , Y , , , s 0), (1). Введем следующее нелинейное преобразование - алгоритм возведения в степень по модулю простого числа [25]:. Тогда алгоритм Ам выполняет инъективное отображение F 3: М 3 → М 3. - для р 1 = 5: H (p 1)= (5-1)=2;. Если в модели (1) нелинейная функция усложнения определена как система (9), то нелинейная функция усложнения выполняет в (1) инъективное отображение (3). n =k· m = H(pa )· m , m = 2, 4, 8, 16, . При m = 4, H 2 = 8, k 2 = n /4, = 8n /4 = 23n /4 ,. нелинейных ПСП с периодом 2n -1.

**Key words part:** 0.5666666666666667

=================================

**Текст:** Тема развития, совершенствования моделей и алгоритмов построения генераторов псевдослучайных последовательностей (ПСП) с характеристиками, близкими к случайным последовательностям, постоянно отражается в публикациях. Примерами подобных работ, опубликованных в последние годы, являются [1–18]. Одной из активно исследуемых задач в этом направлении является задача [19,20] усложнения аналитического строения псевдослучайных последовательностей, применяемых для различных приложений (помехозащищенность широкополосных сигналов, защита информации и др.). Распространенный подход усложнения строения формируемой ПСП заключается в применении к элементам заданной исходной ПСП дополнительного преобразования в виде некоторой нелинейной внешней логики (нелинейной функции усложнения (НФУ)) [6, 19-24].В данном подходе выбором исходнойПСП обеспечивается требуемый максимальный период формируемой псевдослучайной последовательности, а необходимое ее качество определяется моделью НФУ.. Важной задачей в отмеченном подходе является построение математических моделей нелинейной функции усложнения, однозначно выполняющей преобразование исходной ПСП и формирующей выходные нелинейные последовательности, обладающие на заданном максимальном периоде статистическими свойствами, приближающимися к свойствам случайной равновероятной последовательности. Этой задаче посвящена, в частности, работа [24], где представлена модель генератора ПСП с нелинейной функцией усложнения, реализующей усложнение ПСП из класса М- последовательностей [7] путем перестановки ее элементов. Перестановка в [24] реализуется на основе модулярной операции возведения в степень по модулю простого числа Ферма. Данная НФУ позволяет менять строение ПСП параметрически - путем замены в модулярной операции значений первообразных корней [25]. Однако период получаемых нелинейных ПСП на модели [24] ограничен величиной модуля, определяемого простым числом Ферма.. Целью работы является определение и алгоритмическое построение математической модели представления нелинейных ПСП на основе модулярной операции возведения в степень по модулю, принадлежащему к множеству простых чисел Ферма, позволяющей получать нелинейные ПСП с заданными перио­дами L = 2n −1 и L = 2n , где n > 1.. 1.Постановка задачи. Рассмотрим генератор ПСП в виде конечного автономного автомата с функцией выхода:. (S , Y , , , s 0), (1). где S - конечноемножество состояний; Y - конечное множество выходных букв; : S → S - функция переходов; : S → Y - функция выхода; s 0 – начальное состояние. Пусть |S | = |Y |, состояния автомата (1) являются двоичными векторами , выходные буквы являются двоичными векторами . Функция переходов автомата выполняет преобразование вектора Х в вектор Х и реализуется как генератор последовательности де-Брейна с периодом 2n на основе РС с нелинейной функцией обратной связи, определяемой полиномом вида [20]:. , (2). где F (x ) примитивный полином степени n над полем GF(2) = {0, 1}. Полином F (x ) задает функцию обратной связи РС, генерирующего M -последовательность с периодом 2n −1. Функция выхода рассматривается как функция усложнения, выполняющая однозначное отображение. Z = (X): G(2)n → G(2)n, (3). где G(2)n – множество n-мерных двоичных векторов, |G(2)n| = 2n.. Введем следующее нелинейное преобразование - алгоритм возведения в степень по модулю простого числа [25]:. , (4). где p - простое число, j - целое число, Qh - заданный первообразный корень (примитивный элемент) по модулю p , h = 1, 2, …, (p −1) (число первообразных корней при заданном модуле p равно значению функции Эйлера (p−1)) [25], Qh принимает значения из интервала 1 < Qh < p −1.. Отметим следующие свойства алгоритма (4), вытекающие из свойств первообразных корней по модулю p [25]. Обозначим их символами С1, С2, С3. Введем множества М 1 = {1, 2, …, p − 1}, М 2 = {0,1, 2, …, p − 1}.. Свойство С1 [25]. Пусть в алгоритме (4) переменная j принимает значения из множества М 1 = {1, 2, …, p −1}. Тогда алгоритм (4) выполняет инъективное отображение F 1: М 1 → М 1 и последовательность значений у j , получаемая по алгоритму (4), имеет период p −1. Отображение F 1 есть перестановка, заданная на М 1.. Свойство С2 [25]. Пусть в алгоритме (4) переменная j принимает значения из множества М 2 ={0,1, 2, …, p - 1}. Тогда алгоритм (4) выполняет однозначное отображение, сюръекцию F 2: М 2→М 1. В (4) значениям j = 0 и j = p − 1 сопоставляется значение у j = 1.. Свойство С3 [25]. Пусть в алгоритме (4) переменная j принимает значения из множества М 1. Тогда алгоритм (4) при j = (p −1)/2 и заданном Qh , 1 < Qh < p –1, выполняет соответствие вида j→(влечет) у j = р − 1, т.е.. (5). Решаемой задачей является построение для автоматной модели (1) нелинейной функции выхода, реализующей инъективное отображение (3), где n – четное, n > 1, на основе алгоритма (4).. 2. Анализ задачи, подход к решению. Из свойств С1-С3 следует:. 1) для реализации в модели (1) инъективного отображения (3) алгоритмом (4) необходимым условием является выполнение соотношения p > 2n , n > 1;. 2) чем больше величина ∆= p − 2n , тем больше отличается по составу и величине элементов множество Y от S при реализации функции выхода .. Введем в рассмотрение следующее множество простых чисел p , при которых величина ∆ имеет минимальное значение, равное ∆ =1: множество М F ={р 1, р 2, р 3, р 4} простых чисел Ферма (чисел вида р = 2m + 1, где m =2, 4, 8, 16, р 1=22+1=5, р 2=24+1=17, р 3=28+1=257, р 4=216+1=65537).. Введем множество М 3 = {0, 1, 2, …, 2m −1}, |М 3|=2m , m= 2, 4, 8, 16.. Рассмотрим решение задачи реализации инъективного отображения вида F 3: М 3→М 3 на основе алгоритма (4).. Отметим следующее свойство алгоритма (4).. Утверждение 1. Пусть в алгоритме (4) выполняются следующие условия: модуль рМ F , 1 < Qh < p –1, переменная j принимает значения из множества М 3, величина 2m = p −1, m = 2, 4, 8, 16. Тогда алгоритм (4) выполняет инъективное отображение вида. F 2: М 3 → М 4 = {1, 2, …, 2m -1, 2m },. где представлено соответствие. . (6). Справедливость утверждения 1 следует из свойств С1, С2, C3.. Отметим: операцию возведения в степень по модулю рМ F по выражению (4) можно реализовать путем применения вычислительного алгоритма, представленного в виде [26].. Пример 1. Реализация в соответствии с [26] операции возведения в степень по модулю. Пусть m =4, р 2=17, Q 1=3.. 1) Зададим двоичное текущее значение j . Пусть j =(х 0 х 1 х 2 х 3)2= 1011.. 2) Заполним следующую таблицу. j. х 0. х 1. х 2. х 3. Q. б 0. б 1. б 2. б 3. где б 0= Q 1=3 - заданный примитивный элемент по модулю р =17,. , l = 0, 1, 2, 3.. 3) Результат yj = б 3 (двоичный четырехразрядный код) считывается из последней ячейки второй строки. Для j =1011 получим y j = б 3= 0111.. . Обозначим символом Ам алгоритм, являющийся следующей модификацией алгоритма (4): алгоритм Ам отличается от алгоритма (4) только тем, что при рМ F , j = 2m /2 и 1 < Qh < p −1 выполняет вместо соответствия (6) соответствие вида. . (7). Следствие 1 (из утверждения 1). Пусть j в (4) принимает значения из множества М 3, модуль рМ F , 2m = p−1, m = 2, 4, 8, 16 и 1 < Qh < p –1. Тогда алгоритм Ам выполняет инъективное отображение F 3: М 3 → М 3.. Отображение F 3 есть перестановка, заданная на М 3.. Из следствия 1 вытекает следующее:. 1) применение в автоматной модели (1) алгоритма Ам для реализации функции выхода позволяет выполнять инъективное отображение (3), где n = m = 2, 4, 8, 16;. 2) получаемая нелинейная ПСП на выходе НФУ имеет абсолютно максимальный период L = 2n , где n = m = 2, 4, 8, 16 и по своей структуре является перестановкой элементов (векторов Х ) последовательности де-Брейна, формируемой по соотношению (2).. Замечание 1. Число H (pa ), , первообразных корней помодулю рМ F , определяемое функцией Эйлера, равно:. - для р 1 = 5: H (p 1)= (5-1)=2;. - для р 2 = 17: H (p 2)= (17-1)=8;. - для р 3 = 257: H (p 3)= (257-1)=128;. - для р 4 = 65537: H (p 4)= (65537-1)=32768. (8). Применение в алгоритме Ам при фиксированном модуле рМ F различных примитивных элементов Qh позволяет параметрически, меняя Qh в Ам (для каждого периода используется новый элемент Qh ), менять структуру ПСП на выходе алгоритма Ам и получать ансамбль формируемых ПСП, определяемый величиной H(pa ), , представленной в (8).. Отметим: величина периода получаемых ПСП на выходе автоматной модели (1) при реализации НФУ в виде алгоритма Ам , где n = m = 2, 4, 8, 16, ограничена величиной модуля рМ F .. В разделе 3 предлагается представление модели НФУ в виде системы алгоритмов Ам , реализующей инъективное отображение (3), где n - четное, n > 1.. 3. Модель функции усложнения. Примем n ≥ m. Выполним разбиение n - мерного двоичного вектора Х , n ≡0(modm ),m = 2, 4, 8, 16, на k блоков - m −разрядных двоичных векторов Хi , , k = n /m . Подобное разбиение проведем и для вектора Z = (Zi ), . При данном разбиении двоичные вектора Хi и Zi , , принимают значения из множества М 3 = {0,1,2, …, 2m -1}, m = 2, 4, 8, 16.. Введем в рассмотрение кортеж вида. (β1, β2, …, βk) (9). где βi, - однозначное преобразование (инъекция), выполняемое алгоритмом Ам при m = 2, 4, 8, 16 двоичных значений вектора Хi, , по модулю рМ F при заданном Qh , 1 < Qh < p –1, в двоичные значения вектора Zi . Примем n = k · m ≥ H(pa )· m , , m = 2, 4, 8, 16 (данные условия определяют возможность кратного применения в (9) элемента βi , ).. Покажем, что нелинейная функция усложнения в модели (1), представляемая как система (9), при отмеченных ограничениях выполняет инъективное отображение (3).. Утверждение 2 (основное). Если в модели (1) нелинейная функция усложнения определена как система (9), то нелинейная функция усложнения выполняет в (1) инъективное отображение (3).. Справедливость утверждения 2 следует из свойств образов и прообразов для инъективного отображения [27, с. 17].. Систему преобразований (9) будем рассматривать как модель функции усложнения для реализации инъективного отображения (3) в автомате (1).. 4. О величине ансамбля формируемых последовательностей. Применение в преобразованиях βi , , системы (9) при фиксированном модуле рМ F различных примитивных элементов Qh позволяет параметрически (меняя Qh ) менять структуру ПСП на выходе НФУ.. Условия, принятые для системы (9): n = k · m ≥ H(pa )· m , , m = 2, 4, 8, 16 и утверждение 2 определяют разнообразие модификаций реализации системы (9) и получение на основе (1) различных по размеру ансамблей нелинейных ПСП.. Рассмотрим два случая получения ансамблей нелинейных ПСП, определяемые следующими ограничениями, которые накладываются на систему (9).. Примем, что в системе (9) ограничение имеет вид. n =k· m = H(pa )· m , m = 2, 4, 8, 16, . (10). Следствие 2 (из утверждения 2). Пусть в системе (9) при ограничении (10) в преобразованиях βi, , применяются различные элементы Qh , 1 < Qh < p –1, в соответствии с фиксированным модулем рМ F . Тогда для реализации в модели (1) отображения (3) при фиксированном модуле рМ F существует H(pa )!, , различных систем вида (9).. Следствие 2 обосновывает возможность при выполнении ограничения вида (10) в системе (9) получить на выходе автомата (1), при фиксированной функции переходов вида (2), с примитивным полиномом степени n = H(pa )·m , ансамбль Vh = H(pa )! нелинейных псевдослучайных последовательностей с заданным периодом L = 2n , где n = H(pa )·m , .. Пример 2. Пусть для модели (1) в системе (9) с ограничением (10), в элементах βi применяется модуль р 3 = 257, m = 8, k = H(pa ) = 128 и в (2) применяется примитивный полином степени n = H(pa )·m = 1024. Тогда период ПСП на выходе автомата (1) равен L = 21024 и ансамбль Vh = 128!. Нижнюю оценку величины Vh = H(pa )! при m = 16 и n= m· 32768 определим (в соответствии с формулой Стирлинга [28]) значением. Vh = О(232768). (11). Примем, что в системе (9) ограничение имеет вид. n =k· m > H(pa )·m , , m = 2, 4, 8, 16. (12). Для данного случая в качестве иллюстрации простейшего схемного представления НФУ в модели (1), определяемого применением наименьшего модуля р 1 = 5 в элементе βi , рассмотрим следующую последовательностную реализацию системы (9) с ограничением (12).. Пусть в (1) задан период L =2n последовательности де-Брейна, например, n = 128, m = 2, модуль р 1 = 5 и заданы элементы Q 1 = 2 и Q 2 = 3, вектор Х разбит на k = n/m двухразрядных блоков (Хi, ). Преобразование вектора Хi в вектор Zi элементом βi , , назовем раундом. Пусть система (9) содержит только один элемент β, где модуль р 1 = 5. Преобразование вектора Х размера 128 бит в вектор Z размера 128 бит проведем этим элементом β за k=128/2 раундов. В раундах, на периоде 2n , преобразование в элементе β выполняется с чередованием элементов Q 1, Q 2 (хранимыми в отдельной памяти). Пусть динамическое чередование элементов Q 1, Q 2 в каждом раунде производится в соответствии с некоторой дополнительной двоичной ПСП (элементу 0 сопоставляется Q 1, элементу 1 сопоставляется Q 2) генерируемой дополнительным генератором с периодом L 1=k =64, определяемым числом раундов. В частности, таким генератором может быть генератор де-Брейна , подобный рассмотренному выше, с периодом L 1 =64. В этом случае число возможных, дополнительных ПСП равно 2k = 264, что позволяет получить на выходе НФУ при модуле р 1 = 5 ансамбль нелинейных ПСП, имеющих период L = 2n , n = k · m , размером V 1=2k = .. В подобной последовательностной реализации схемы НФУ с увеличением модуля рМ F размер ансамбля формируемых последовательностей можно увеличить. С этой целью преобразование β в раундах по модулю рМ F выполняется динамическим чередованием элементов Qh из множества первообразных корней мощности Ha = H (p a), . Чередование в раунде выполняется в соответствии с некоторой дополнительной Ha -значной ПСП, генерируемой дополнительным генератором ПСП с периодом L = ki =n /mi , mi =4, 8, 16, где ki > Hi , i = a = 2, 3, 4. Используемые в раунде элементы Qh хранятся в отдельной памяти емкостью Hi , i = 2, 3, 4 , mi -разрядных ячеек.. Рассмотренная схема реализации НФУ позволяет получить следующие размеры ансамблей , i = 2, 3, 4, формируемых нелинейных последовательностей периода L = 2n .. При m = 4, H 2 = 8, k 2 = n /4, = 8n /4 = 23n /4 ,. при m = 8, H 3 = 128, k 3 = n /8, = 128n /8=27n /8,. при m = 16, H 4 = 32768, k 4 = n /16, = 32768n /16=215n /16. (13). 5. Автоматная модель формирования. нелинейных ПСП с периодом 2n -1. Рассмотрим следующий частный случай автоматной модели (1), позволяющий получать нелинейные ПСП с периодом 2n −1.. Пусть функция : S → S переходов определяемого автомата реализуется регистром сдвига с характеристическим примитивным полиномом F (x ) степени n . Состояния автомата являются двоичными векторами , выходные буквы являются двоичными векторами . Полином F (x ) задает функцию линейной обратной связи РС, генерирующего М -последовательность с периодом 2n -1. В М -последовательности отсутствует состояние (вектор Х ) из n нулей, которое обозначим как вектор Х 0. Функция выхода рассматривается как функция усложнения, выполняющая инъективное отображение. : S → Y , |S |=|Y | =2n −1. (14). Данную модификацию конечно-автоматной модели (1) обозначим символом КАY .. Рассмотрим задачу построения для автомата КAY математической модели нелинейной функции выхода, реализующей инъективное отображение вида (14) на основе алгоритма (4) и позволяющей получить выходную нелинейную ПСП с заданным перио­дом L =2n −1, где n ≡ 0(mod m ),m = 2, 4, 8, 16, n > m .. Представление модели требуемой нелинейной функции усложнения для автомата КAY определим на основе системы преобразований (9) при ограничениях (10) и (12).. Примем: в системе (9) ограничение имеет вид (10); преобразование βi, , в (9) выполняется алгоритмом Ам , где двоичные вектора Хi и Zi принимают значения из множества М 3 ={0,1,2, …, 2m −1}.. Возможность реализации НФУ в модели КАY на основе системы (9) при ограничении (10) обосновывает. Следствие 3 (из утверждения 2). Если нелинейная функция усложнения определена как система (9) с ограничением (10), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y.. Примем: в системе (9) ограничение имеет вид (12).. Возможность реализации НФУ в модели КАY на основе системы (9) при ограничении (12) обосновывает. Следствие 4 (из утверждения 2). Если нелинейная функция усложнения определена как система (9) с ограничением (12), то НФУ в модели КАY выполняет инъективное отображение (14), и где S не равно Y.. Замечание 2.При реализации в КАY системой (9) отображения при ограничениях (10) и (12) получаемое множество Y отличается от множества S двумя n -разрядными векторами: Y включает нулевой вектор Z – вектор Z 0, все n разрядов которого содержат значение 0 и не содержит вектор Z =(Z i ), где у m - разрядного вектора Z i , , m =2, 4, 8, 16, младший разряд содержит значение 1.. Вектор Z 0 включен в Y в силу следствия 1. Вектор Z =(Z i ), , не содержится в Y вследствие того, что множество S не содержит вектор Х 0, которому алгоритм Ам ставит в соответствие данный вектор Z = (Z i ).. ПСП, получаемую на выходе автомата КАY , будем рассматривать как квазиподобную М -последовательности по статистическим (частотным) свойствам на периоде 2n −1.. Пример 3.Преобразование М-последовательности системой (9) вида (β1, β2).. Пусть n = 4, р = 5, m = 2, k = 2 система (9) представлена парой преобразований (β1, β2), где β1 выполняется с Q 1=3 и β2 выполняется с Q 2 = 2 и функция переходов автомата КАY формирует последовательность векторов Х , принимающих следующие 15 различных четырехразрядных двоичных значений в соответствии с М-последовательностью, построенной на РС с s0 = 1000, по примитивному полиному f(x )=x 4+x +1: (1000, 0100, 0010, 1001, 1100, 0110, 1011, 0101, 1010, 1101, 1110, 1111, 0111, 0011, 0001). Тогда на выходе НФУ, представленной парой преобразований (β1, β2), будет получена следующая последовательность четырехразрядных двоичных векторов Z с периодом L =15: (0001, 1101, 0100, 0010, 1001, 1100, 0011, 1110, 0000, 1010, 1000, 1011, 1111, 0111, 0110). В данной последовательности имеется вектор 0000 и отсутствует вектор 0101, что соответствует замечанию 2.. Отметим: размеры ансамблей, получаемые на модели КАY определяются соотношениями (11) и (13).. Заключение. 1. Представленная автоматная модель формирования нелинейных псевдослучайных последовательностей с заданными периодами L = 2n и L = 2n −1, где n> 1, n ≡ 0 mod m , m =2,4,8,16, отличается видом модели функции выхода, задаваемой системой, реализующей k = n /m нелинейных операций возведения в степень по модулю, принадлежащему к множеству простых чисел Ферма и выполняющей инъективное преобразование.. 2. Определены и аналитически обоснованы алгоритмические возможности автоматной модели (утверждения 1 и 2, следствия 1 и 2), определяющие вид аналитического усложнения ПСП на периоде L = 2n : функция выхода автомата выполняет на основе нелинейных модулярных операций псевдослучайную перестановку элементов (векторов Х ) последовательности де-Брейна.. 3. Определены и аналитически обоснованы алгоритмические свойства автоматной модели (следствие 3, следствие 4), определяющие аналитическое усложнение ПСП на периоде L = 2n −1: функция выхода автомата порождает на основе нелинейных модулярных операций нелинейную ПСП, квазиподобную М -последовательности по статистическим (частотным) свойствам на периоде 2n −1.. 4. В автоматной модели достигается дополнительное изменение структуры выходных ПСП путем псевдослучайной перестановки в модулярных операциях значений первообразных корней.. 5. Нижняя оценка размера ансамбля Vh = H(pa )! при m = 16 и n= m· 32768 определяется значением Vh =О(232768).