

МЕТОДИКА СОЗДАНИЯ ГЕНЕРАТОРОВ ПЕРИОДИЧЕСКИХ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

степени удовлетворяющие п. 1.

Найденные коэффициенты позволяют построить ОЛУФП, решения которого представляют собой массивы периодических булевозначных последовательностей. Они могут использоваться в генераторах псевдослучайных битов, применяемых при защите банковских информационных систем.

Литература: 1. Анин Б. Ю. *Защита компьютерной информации*. - СПб.: БХВ - Санкт-Петербург. - 2000. - 384 с. 2. Зегжда Д. П., Ивашко А. М. *Основы безопасности информационных систем*. - М.: Горячая линия – Телеком, 2000. - 452с. - С. 241 - 254. 3. Б. Шнайер. *Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си*. - М.: Триумф, 2002. 4. J. M. Carroll, L. E. Robbins. *Using binary derivatives to test an enhancement of DES //Cryptologia*. - 1988. - V. 12. - № 4. - Pp. 193 - 208. 5. Березюк Н. Г., Холодный М. Ф. *Булевы дифференциальные уравнения и методы их решения*. - В сб.: *Математическое и программное обеспечение задач оптимизации технических систем*. - Киев. - "Наукова думка". - 1987. - С. 61 - 65. 6. В. Н. Куценко, Т. В. Левченко, В. В. Мясоедов. *Модель цифровой подписи/Захист інформації в Україні*. - Спеціальний випуск № 22. - С. 29 - 35. 7. В. Мясоедов. *Золотое сечение в шифровании данных*// В сб.: *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. - Науково-технічний збірник. - Випуск 4. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2002. - 213 с. - С. 105. 8. В. Мясоедов, В. Куценко, *Оценка случайности по избыточности* // В сб.: *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. - Науково-технічний збірник. - Випуск 8. - К.: НДЦ "Тезіс" НТУУ "КПІ". - 2004. - 166 с.- С. 90 - 94.

УДК 681.3.067:681.3.016

ОЦЕНКА АСИММЕТРИИ ПО АВТОКОРРЕЛЯЦИИ

Геннадий Куценко

КП НТК «Импульс»

Аннотация: На примере псевдослучайной последовательности генератора Фибоначчи подробно описаны результаты экспериментального исследования асимметрии методами автокорреляции. Введенный в статье коэффициент ранговой упорядоченности двоичных слов из полезной длины периода последовательности в рассмотренном примере очень мал.

Summary: On example of the pseudorandom sequence of Fibonacci generator in detail described results of the experimental study to asymmetries by methods of autocorrelation.

Ключевые слова: Генератор Фибоначчи, псевдослучайные числа, асимметрия последовательностей, автокорреляционная функция, ранговая корреляция, ранговая упорядоченность.

Известные методы оценки качества псевдослучайных последовательностей «в целом» [1] являются недостаточными, так как их применение не гарантирует отсутствия простых симметрий – повторений отрезков последовательности – в псевдослучайных последовательностях, порождаемых определёнными алгоритмами. Это недопустимо с точки зрения применений псевдослучайных последовательностей в области защиты данных.

Удобным инструментом локальных оценок, в частности для проверки отсутствия простых симметрий в псевдослучайных последовательностях, является вычисление автокорреляционной функции, малые значения которой несовместимы с наличием в последовательностях простых симметрий. Это выражено как постулат в [2]. Имеется также средство оценки бинарных последовательностей, позволяющее локализовать вычисления автокорреляционной функции, трактуемой как совокупность коэффициентов корреляции отрезков последовательности, попадающих в пару подвижных «окон» одинакового размера. Отсутствие простых симметрий в псевдослучайной последовательности может быть проверено с помощью оценок автокорреляции и в более широком случае, когда ко второму экземпляру последовательности применён некоторый простой оператор. Кроме того, автокорреляционные схемы оценки асимметрии могут быть применены также при минимальных предположениях о свойствах шкалы генерируемых объектов – тогда необходимо вычислять ранговые корреляции [3].

Теоретические средства локального оценивания хотя и возможны, но всегда ориентированы на конкретные алгоритмы генерации. При этом весьма полезны предварительные эмпирические исследования.

Предметом подробного рассмотрения в статье являются результаты экспериментальных исследований асимметрии методами автокорреляции на примере псевдослучайных последовательностей двоичных слов, порождаемых генератором Фибоначчи.

Генератор Фибоначчи может быть реализован как последовательное длинное двоичное сложение с парой начальных значений в ограниченной разрядной сетке.

Период сплошной последовательности генератора Фибоначчи равен $3 \cdot 2^{L-1}$, а период скрытой части операндов, определяющий полезную длину периода – $3 \cdot 2^{L_h-1}$. Периоды соответствующих подпоследовательностей нечётных операндов сплошной последовательности – 2^L и 2^{L_h} .

При вычислении автокорреляционной функции периодических последовательностей естественным является сдвиг второго экземпляра последовательности за конец периода относительно первого экземпляра.

Требуется экспериментально проверить возможность исключения гипотез о наличии простых симметрий и/или антисимметрий в примерах подпоследовательностей двоичных слов с помощью вычисления автокорреляционной функции, а именно: вычислить значения стандартной функции автокорреляции в пределах полного периода в прямом и обратном порядке последовательностей двоичных слов, трактуемых как числа.

Такие же экспериментальные оценки требуется получить в двухоконной автокорреляционной схеме для прямых и обратных подпоследовательностей двоичных слов в пределах полезной длины периода, определяемой как длина периода скрытой части операндов.

Для последовательности битов переполнения (однобитовых двоичных слов) требуется вычислить ранговые (логические) функции автокорреляции в двухоконной схеме, причём кроме прямых и обратных последовательностей битов требуется экспериментально оценить обобщённую функцию автокорреляции с последовательностями битов, получаемых из рассматриваемых с помощью оператора булева отрицания.

В численных экспериментах использована последовательность нечётных операндов длины $N = 2^{19}$ и двоичные слова длиной $L_w = 8$ при длине скрытой части операндов $L_h = 11$ с начальными значениями $N_{-1} = 88907$, $N_0 = 145545$.

Вычисление автокорреляционной функции в однооконной схеме автокорреляции производилось с учётом независимости среднего значения $M(w)$ и вариации $V(w)$ периодической последовательности w двоичных слов в полном периоде от выбора начала второго экземпляра этой последовательности (в силу

$$\text{доказанной выше теоремы) по формуле } A_{cf}(k) = \frac{\sum_{m=0}^{N-1} w_m w_{k+m} - NM(w)^2}{N \cdot V(w)} .$$

На рис. 1 приведены графики автокорреляционной функции для интервала смещений $1..2^{10}$ и её выборочные значения в полном периоде для смещений $2^{10}, 2 \cdot 2^{10}, \dots, 2^{19} - 2^{10}$

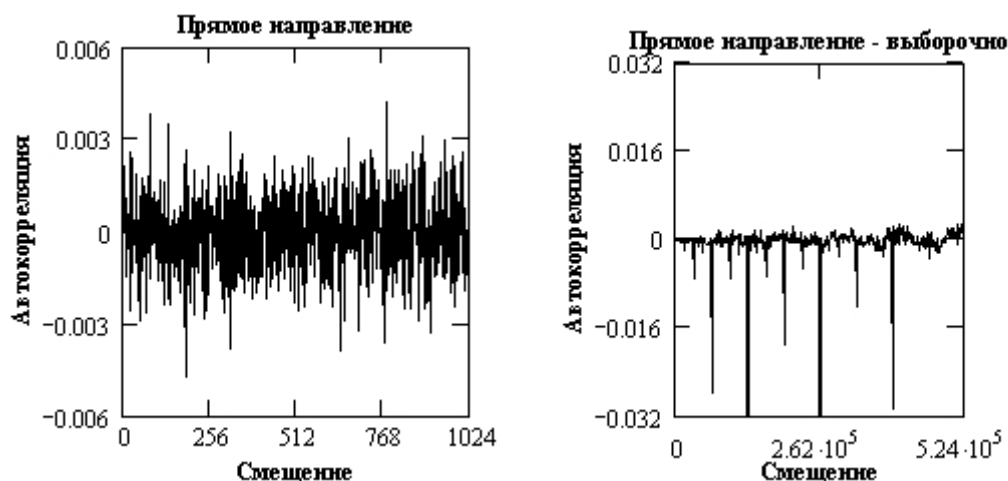


Рисунок 1 – Эмпирический график автокорреляционной функции

На втором из приведенных графиков аномальные значения автокорреляционной функции -0.094 и -0.252 при смещениях 2^{17} и 2^{18} не показаны. Обращает на себя внимание регулярность всплесков

значений функции вблизи половины, четверти, ... периода, хотя сами значения «невелики». Причиной этого явления, по-видимому, является логическая антисимметрия последовательностей сумм битов переполнения по модулю 2 в каждой позиции внутри двоичного слова. При этом вклад логической антисимметрии сумм битов переполнения в автокорреляционную функцию убывает при сдвиге позиции вправо.

Описанное явление не имеет места при вычислении автокорреляционной функции в противоположных направлениях последовательности (рис. 2), хотя на втором из графиков этого рисунка заметен тренд роста размаха колебаний автокорреляционной функции в зависимости от длины участка «перекрытия» прямой и обратной последовательностей.

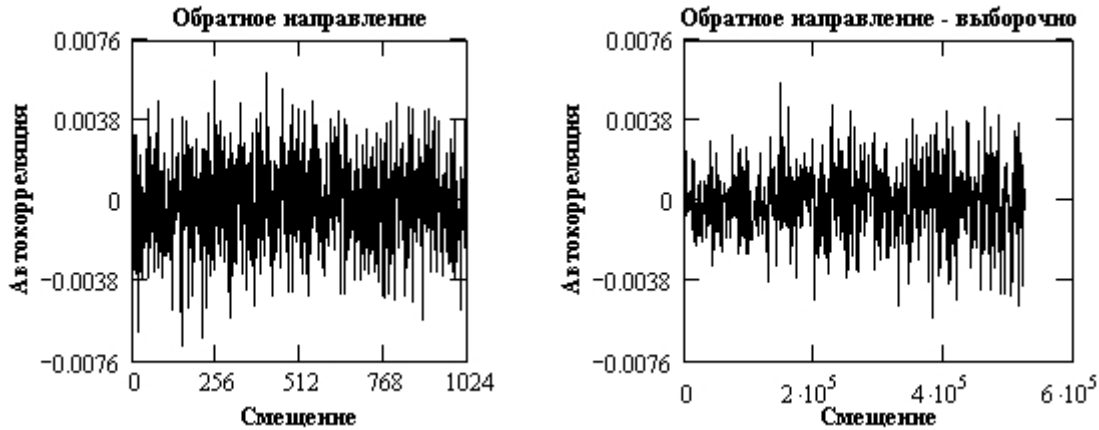


Рисунок 2 – Эмпирическая проверка простой асимметрии

Отмеченное выше anomalous поведение автокорреляционной функции при некоторых смещениях побуждает ограничить исследование асимметрии последовательностей двоичных слов нечётных операндов полезной длины периода $N = 2^{11}$. Так как последовательность в этом случае уже не периодична требуется применение двухоконной автокорреляционной схемы

$$Acf_2(0, k) = \frac{\sum_{m=0}^{N_1-1} w_m w_{k+m} - N M_0(w) M_k(w)}{N \cdot \sqrt{V_0(w) V_k(w)}}$$

Размер окон выбран равным $N_1 = 2^9$ – четверти полезной длины периода, а интервал смещений автокорреляционной функции – $1, 2, \dots, 2^{11} - 2^9$. Графики автокорреляции показаны на рис. 3.

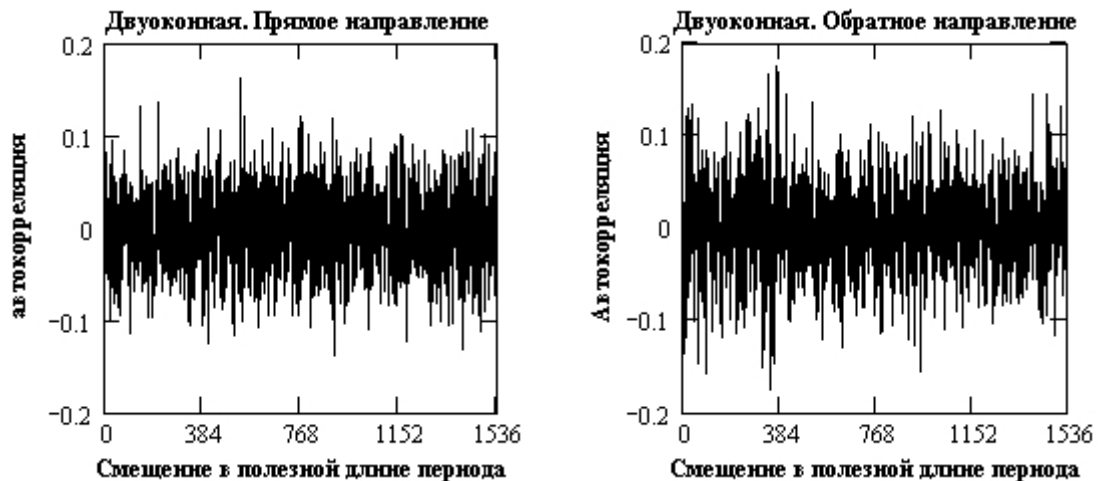


Рисунок – 3 Пример двухоконной автокорреляции в полезной длине периода

Из приведенного примера видно, что двухоконная автокорреляционная функция не выказывает

аномального поведения. Увеличение максимальных отклонений автокорреляционной функции по сравнению с графиками рис. 1 и рис. 2 может быть объяснено ослаблением «сглаживающего эффекта» при уменьшении размера окон вычисления автокорреляционной функции (этот сглаживающий эффект хорошо заметен при вычислении автокорреляционной функции пилообразного напряжения; в этом случае автокорреляционная функция пары линейных зубцов является параболой, «острота», т. е. фокальное расстояние, которой уменьшается при увеличении длины периода пилообразного напряжения с соответствующим увеличением размера окна, равного длине периода).

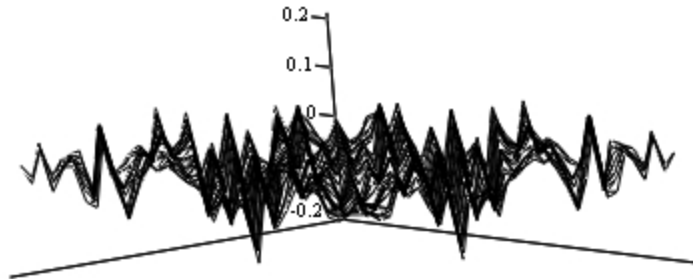


Рисунок 4 – Пример двухоконной автокорреляции

Отсутствие аномалий имеет место и для полной автокорреляционной функции $Acf_2(j, k)$ при $0 < j < k$, показанной на рис. 4 (после 16×16 -кратного прореживания графика; $Acf_2(j, j)$, равное 1 на диагонали графика, показано как нулевое для наглядности). Незначительный тренд размаха колебаний функции автокорреляции в направлении к диагонали, по-видимому, объясним длиной участка перекрытия окон, где сказывается суммарный вклад одинаковых сумм битов переполнения по модулю 2 внутри двоичного слова.

Явление трендов побуждает рассмотреть двухоконную автокорреляцию сумм битов переполнения по модулю 2 в пределах полезной длины периода.

Двоичные слова до некоторой степени можно трактовать как целые числа, что позволяет применить обычный способ вычисления коэффициента корреляции. Для битовых последовательностей такая трактовка не имеет смысла в силу «бедности» свойств булевой шкалы [0,1]. (Заметим при этом, что замена арифметических операций логическими – с модулем 2^{L-w} – в статистических вычислениях приводит к тому, что средние и вариации могут оказаться нулевыми одновременно. Это делает проблематичным построение критериев для проверки гипотез). Минимальным свойством шкалы, помимо единственности наименований, является её упорядоченность – определение для каждого элемента определённого ранга. Поэтому в автокорреляционных схемах для сумм битов по модулю 2, то есть для однобитовых двоичных слов, применено вычисление коэффициента ранговой корреляции Кендалла [4]. Биту '0' приписан ранг 0, биту '1' – ранг 1, так что '0' < '1'. Ранговая статистика представлена коэффициентом корреляции Кендалла между вектором рангов элементов выборки и вектором порядковых номеров элементов выборки

$$\tau = \frac{1}{N(N-1)} \sum_{i \neq j} \text{sign}(i - j) \text{sign}(R_i - R_j), \quad (1)$$

где функция sign фиксирует возможные отношения рангов - «больше», «меньше» или «равно». Соответственно для пары наблюдаемых признаков x, y коэффициент корреляции Кендалла, отличающийся от классического, имеет вид

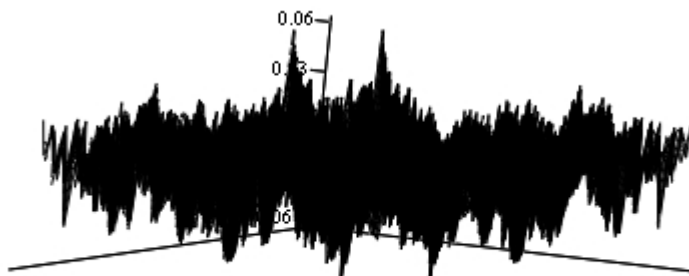
$$\tau_{x,y} = \frac{1}{N(N-1)} \sum_{i \neq j} \text{sign}(R_{x_i} - R_{x_j}) \text{sign}(R_{y_i} - R_{y_j})$$

и может быть вычислен в схеме двухоконной автокорреляции по рангам, определённым выше. (Возможность внешнего определения рангов в формуле (1) для пар значений разнородных признаков $\{x_i, y_i\}$ нами не рассматривается.)

Результат вычисления двухоконной ранговой автокорреляции

$$Acf_{rang}(j, k) = \frac{2}{N(N-1)} \sum_{m < mm} (b_{j+m} - b_{j+mm}) (b_{k+m} - b_{k+mm})$$

для однобитовых двоичных слов b_i (фактически – сумм битов переполнения скрытой части) показан на рис. 5 с 16×16 -кратным прореживанием графика и обнулением $\text{Acf}_{\text{rang}}(j, j)$ на диагонали графика для наглядности. На этом рисунке видно, что значения автокорреляционной функции намного меньше, чем соответствующие значения, вычисленные раньше для 8-битовых двоичных слов, причём регулярность (гладкость) поверхности на графике также значительно уменьшилась, что объяснимо «большой» дискретностью булевой шкалы по сравнению с численной.



ff

Рисунок – 5 Пример двухоконной ранговой автокорреляции однобитовых слов

Аналогичные результаты (рис. 6) получены в двухоконной схеме ранговой автокорреляции для обратного направления второго окна и комбинаций направлений с операцией булева отрицания во втором окне

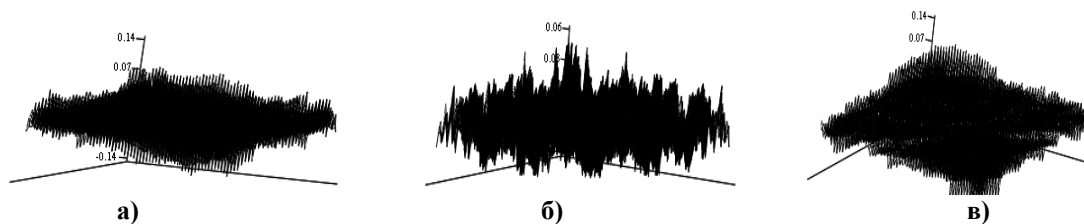


Рисунок 6 – Варианты двухоконной ранговой корреляции однобитовых слов
а) обратное направление ± 0.14 ; б) прямое направление с булевым отрицанием ± 0.06 ;
в) обратное направление с булевым отрицанием ± 0.14

На рис. 6 видно, что интервал значений функции ранговой автокорреляции в противоположных направлениях – а) и в) - шире, чем интервал на рис. 5, а поверхности графиков более «пушистые». По-видимому, это может быть объяснено вкладом логической антисимметрии старших однобитовых двоичных слов скрытой части операндов. Дополнительным объяснением наблюдаемых трендов размаха колебаний автокорреляции может служить «связность» последовательности двоичных слов, определяемая алгоритмом генерации.

Проявление тонких явлений симметрии на рис. 1 имеет место и тогда, когда длина периода не кратна длине окна. Во всех случаях нерегулярность функции автокорреляции (отсутствие значительных гладких компактных трендов) свидетельствует об отсутствии простых симметрий в псевдослучайных последовательностях генератора Фибоначчи.

Качественная оценка асимметрии последовательностей двоичных слов приводит к необходимости количественного анализа наблюдаемых тонких явлений когерентности битовых последовательностей и количественной проверки гипотез о независимости сплошных выборок, попадающих в окна автокорреляционной схемы, что выходит за рамки статьи. Такая гипотеза может быть проверена на основе рангового критерия, опирающегося на предположение о нормальном распределении коэффициента ранговой корреляции, которое вовсе не гарантировано в условиях полной представительности выборок.

Коэффициент ранговой корреляции, представленный формулой (1), может быть применён и к одному наблюдаемому признаку. В этом случае он является неклассической мерой упорядоченности, то есть *коэффициентом ранговой упорядоченности* последовательности и может быть применён к

псевдослучайным последовательностям двоичных слов с рангами $0, 1, \dots, 2^{L_w} - 1$. Нулевое значение коэффициента ранговой корреляции соответствует «вполне неупорядоченным» выборкам. Результаты численных экспериментов в пределах полезной длины периода при длине окна 2^9 с введенной нами мерой упорядоченности последовательности 8-битовых двоичных слов относительно «натурального» порядка в окне, $\mu(k) = \frac{-2}{N(N-1)} \sum_{i < j} \text{sign}(w_i - w_j)$, приведены на рис. 7.



Рисунок – 7 Ранговая неупорядоченность последовательности двоичных слов

Эти результаты также свидетельствуют об отсутствии простых симметрий – повторений отрезков последовательности – в пределах полезной длины периода. Ранговая упорядоченность последовательности двоичных слов в пределах полезной длины периода (размер окна 2^{11}) в рассматриваемом примере равна 0.0042.

Таким образом, в рассмотренном примере проявляются тонкие явления симметрии, а простые симметрии не имеют места. В [5] для генератора Фибоначчи доказана теорема о том, что в последовательности может быть не более двух одинаковых подряд идущих двоичных слов (кроме байтов 0 и 255). Представляют интерес теоретические оценки максимальной длины повторяющегося отрезка псевдослучайной последовательности генератора Фибоначчи.

Література: 1. В. Мясоедов, В. Куценко, Оценка случайности по избыточности. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Випуск 8. - К. - 2004. - 166 с. - С. 90. 2. Guang Gong, Member, IEEE, and Amr M. Youssef, Cryptographic Properties of the Welch–Gong Transformation Sequence Generators. IEEE Transactions on information theory/ - vol. 48. - no. 11. - november 2002. - p. 2837. 3. Кендалла коэффициент ранговой корреляции. Математическая энциклопедия. - т. 2. - Москва: «Советская энциклопедия». - 1979. - 1104 с. - С. 846. 4. В. В. Мясоедов, Золотое сечение в шифровании данных. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Випуск 4. - К.: НТУУ.-2002. - 214с. - С. 105.

УДК 517.962.27, 004.056.55

О ВОЗМОЖНОСТЯХ ИСПОЛЬЗОВАНИЯ АРИФМЕТИКИ ФИБОНАЧЧИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Виктория Уфимцева

Харьковская национальная академия городского хозяйства

Аннотация: В статье рассматривается целесообразность использования аппарата арифметики Фибоначчи в области криптографии. Показана перспективность этого направления исследований в рамках совершенствования статистических показателей симметричных криптографических преобразований информации.

Summary: Advisability of application the arithmetic of Fibonacci to cryptography is consider in the article.