використовують обидва методи наведені в табл. 2. Результати порівняння наведені в секундах, бо вказана операція вже є операцією верхнього рівня та час її виконання помітний для користувача.

Таблиця 2 – Результати оцінки швидкості алгоритмів скалярного множення, що використовують метод множення елементів поля [1] та розробленого методу множення елементів

Тип множення	Довжина поля m		
	163	233	431
З використанням класичного варіанту алгоритму множення	$\approx 3{,}015$	$\approx 6{,}345$	$\approx 40{,}3$
Модифікований алгоритм	$\approx 0{,}172$	$\approx 0{,}334$	$\approx 1{,}553$
Перевага модифікованого методу	$\approx 17{,}5$	$\approx 18{,}99$	$\approx 25{,}94$

Висновки

Аналіз алгоритмів виконання операцій множення елементів у нормальному базисі показав, що навіть у найкращих алгоритмів, розроблених для реалізації за допомогою програмних засобів, швидкість виконання множення значно менша, ніж у алгоритмів множення елементів в поліноміальному базисі. Зважаючи на велику кількість рекомендацій щодо використання нормального базису, у тому числі і в укрїнських нормативних документах, можна сказати, що задача удосконалення алгоритмів для нормального базису стоїть досить гостро. Тому авторами було виконано аналіз існуючих алгоритмів виконання елементарних операцій. Аналіз виявив найбільш швидкі алгоритми виконання операцій в нормальному базисі. Огляд цих алгоримів виявив деякі недоліки цих алгоритмів, особливо, алгоритму множення елементів, а також методи та напрямки їх удосконалення. В статті зроблена спроба провести модифікацію алгоритму множення елементів у нормальному базисі, запропонованому в [1]. Удосконалення досягнуті за рахунок як програмної оптимізації, так і алгоритмічної оптимізації. Теоретичні аналізи швидкодії алгоритмів показали, що можливе збільшення швидкості сягає розміру машинного слова систем, для яких розробляється реалізація. Практичні дослідження показали, що середнє збільшення швидкості виконання як операції множення елементів, так і операції скалярного множення сягає 15-26 разів, що є достатньо високим показником.

Література: ***1.*** *IEEE P 1363-2000. Standard Specification for public key cryptography. 2000.* ***2.*** *American National Standard X9.62-1999. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 1999.* ***3.*** *American National Standard X9.63-2000. Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography. 2000.* ***4.*** *ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves. Part 1. Key establishment.* ***5.*** *D. V. Bailey and C. Paar, Optimal Extension Fields for Fast Arithmetic in Public- Key Algorithms, Advances in Cryptology, CRYPTO '98, Lecture Notes in Computer Science 1462, pp.472-485, Springer, 1998.* ***6.*** *Eun Jeong Lee, Duk Soo Kim, Pil Joong Lee. Speed-up of* $F(p^m)$ *Arithmetic for Elliptic Curve Cryptosystems. In Proceedings of ICICS '98, Berlin, 1998. Springer Lecture Notes in Computer Science.* ***7.*** *ДСТУ 4145-2002 „Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка” – К. Держстандарт України, 2003. – 94 с.* ***8.*** *Lidl.R, Niederreiter “Finite fields”, Addison-Wisley, Reading M.A.1983,* ***9.*** *Itoh, Tsujii, “A fast algorythm for computing multiplicative inverses in* $GF(2^m)$ *using normal Bases”*

УДК 681.3.067:681.3.016

МАРКОВСКИЙ ГЕНЕРАТОР ДВОИЧНЫХ ВЕРОЯТНОСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Тарас Левченко
Национальный банк Украины

Аннотация: **Предложен алгоритм двухпараметрического генератора двоичных вероятностных последовательностей на основе цепи Маркова. По результатам проведенного численного моделирования даны рекомендации по выбору параметров для синтеза требуемого генератора.**
Summary: **There is offered algorithm of the two-parametrical generator for binary probabilistic sequences**

on the basis of Markov sequences. There are proposed recommendations based on results of numerical modelling for the of parameters choice for synthesis of required generator.
Ключевые слова: **Цепи Маркова, двоичные псевдослучайные последовательности, корреляция.**

Проверка качества функционирования транспортных протоколов информационных систем в банковской сфере Украины на реальных сетях связи весьма проблематична из-за функциональных особенностей он-лайнового режима. В то же время вопросы безопасности реальных сетей вынуждают разработчиков систем банковской связи и службы их эксплуатации искать способы их проверки на основе имитационного численного моделирования [1]. При решении этих вопросов возникает необходимость применения двоичных вероятностных последовательностей (ДВП), принимающих в каждый момент времени t_k значения 0 либо 1 с вероятностями соответственно q_0 и q_1 при выполнении соотношения

$$q_0(k) + q_1(k) = 1. \tag{1}$$

Известные генераторы [2 и др.] не позволяют создавать коррелированные ДВП. Поэтому разработка генераторов ДВП с заданными вероятностными характеристиками является актуальной.

Цель работы – создание методологической основы для разработки генератора ДВП с заданными вероятностными характеристиками.

Для решения поставленной задачи предлагается использовать генератор ДВП, построенный на основе регулярной цепи Маркова с двумя состояниями ’0’ и ’1’. Регулярная матрица переходов для момента времени t с учетом (1) будет иметь вид

$$P = \begin{bmatrix} q_{00} & 1-q_{00} \\ 1-q_{11} & q_{11} \end{bmatrix} \tag{2}$$

где q_{00} = const, q_{11} = const - соответствующие переходные вероятности.

Представляет интерес статистический анализ выходных ДВП генератора, далее обозначемых β, при изменении параметров q_{00}, q_{11}.

На рис. 1 показан алгоритм генератора.

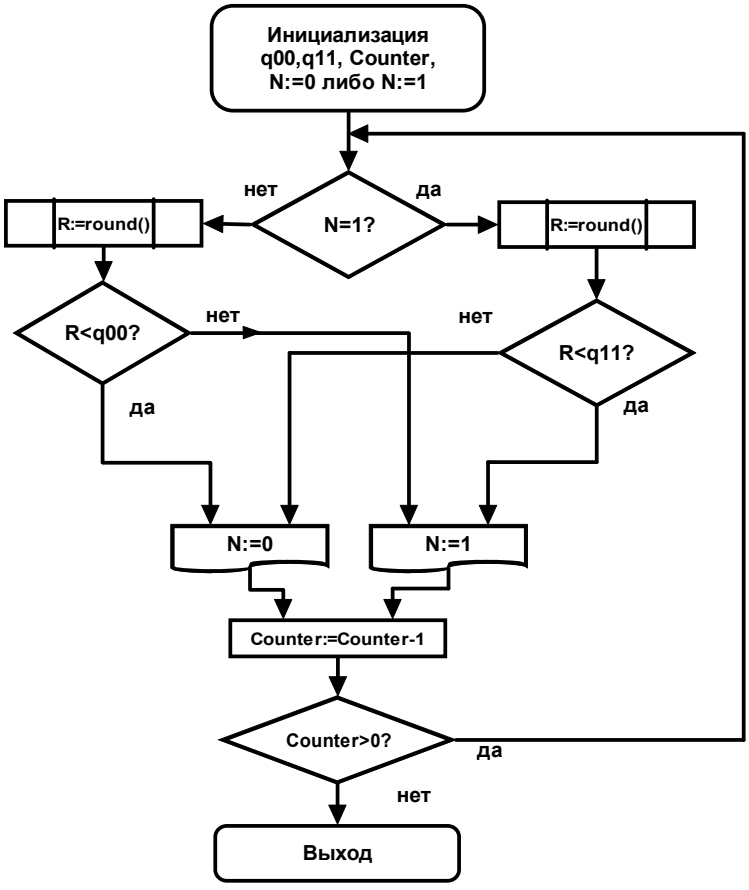


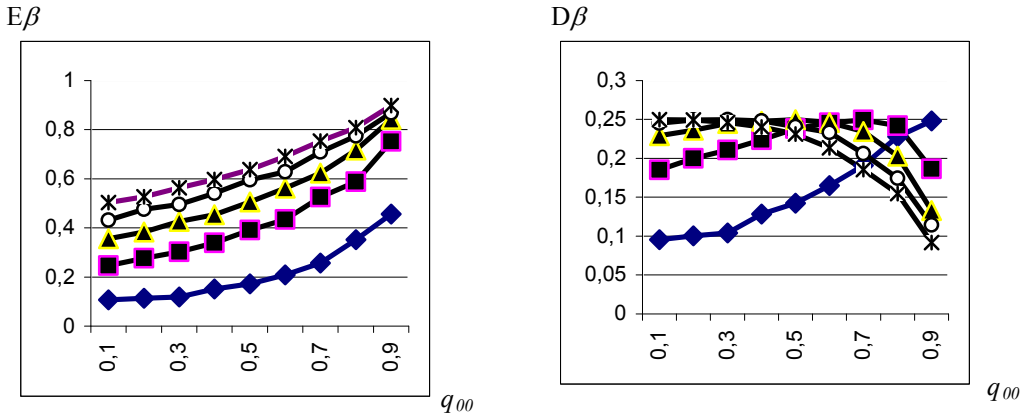
Рисунок 1 – Алгоритм генератора ДВП

В ходе инициализации случайным образом с вероятностью 0,5 определяется начальное значение выходной ДВП N:=0 либо N:=1, задаются значения q_{00} , q_{11} и счетчика числа выходных битов *Counter*. Затем на очередном шаге определяется значение вспомогательной псевдослучайной величины R=*round()*, где *round()* – функция, возвращающая значение равномерно распределенной псевдослучайной величины. При этом q_{00} и q_{11} являются решающими константами для определения значения выходной ДВП N:=0 либо N:=1. Полученное значение N будет исходным для вычислений на следующем шаге. Вычисления продолжаются до обнуления *Counter*.

Генератор был смоделирован в электронных таблицах Excel. В качестве функции *round()* применялся встроенный линейный генератор компилятора Visual Basic. Для анализа использовались выходные последовательности длиной 1000 бит. Осреднение производилось по 10 реализациям выходных последовательностей.

На рис. 2 по оси ординат показаны математическое ожидание Eβ (*а*) и дисперсия Dβ (*б*) выходных ДВП β для разных значений q_{00} и q_{11} (q_{00} отложено по оси абсцисс). Нетрудно видеть, что из-за специфики выходной ДВП ее математическое ожидание и момент 2 порядка равны по величине. Следовательно, дисперсия

$$D\beta = E\beta^2 - (E\beta)^2. \qquad (3)$$



а *б*

Рисунок 2– Математическое ожидание (*а*) и дисперсия (*б*) выходных ДВП: ромб - q_{11} = 0,9, квадрат - q_{11} = 0,7, треугольник - q_{11} = 0,5, кольцо - q_{11} = 0,3, звездочка - q_{11} = 0,1

Анализируя результаты моделирования, можно отметить следующее.

1 При фиксированном q_{00} и увеличении q_{11} математическое ожидание ДВП Eβ монотонно убывает, что свидетельствует об уменьшении относительной доли единиц.

2 Математическое ожидание ДВП при $q_{00} = q_{11}$ оказывается близким к 0,5, что является признаком примерного равенства количеств нулей и единиц.

3 При фиксированном q_{11} и увеличении q_{00} математическое ожидание ДВП монотонно возрастает, что свидетельствует об увеличении относительной доли единиц.

Для нахождения $E\beta$ можно применить классический вероятностный подход, просуммировав математические ожидания возможных выходных ДВП по пространству элементарных событий. В соответствии с приведенным на рис. 1 алгоритмом примем вероятность появления первого знака, равной 0,5.

Построим пространство элементарных событий из всех возможных марковских цепей для разных длин выходных последовательностей и подсчитаем их вероятности по матрице переходов (2). После раскрытия громоздких скобок получим сведенные в таблицу формулы для $E\beta$ в зависимости от длины выходной ДВП.

Таблица

Длина ДВП, бит	Формула для математического ожидания $E\beta$
2	$0{,}5 + (q_{11} - q_{00})/4$
3	$0{,}5 + (q_{11} - q_{00} + q_{11}^2 - q_{00}^2)/6$
4	$0{,}5 + (2q_{11} - 2q_{00} + q_{00}q_{11}^2 - q_{00}^2 q_{11} + q_{11}^3 - q_{00}^3)/8$
5	$0{,}5 + (2q_{11} - 2q_{00} + 2q_{11}^2 - 2q_{00}^2 - q_{11}^3 + q_{00}^3 + q_{11}^4 - q_{00}^4 - q_{00}q_{11}^2 + q_{00}^2 q_{11} - 2q_{00}^3 q_{11} + 2q_{00}q_{11}^3)/10$
6	$0{,}5 + (3q_{11} - 3q_{00} + 3q_{11}^3 - 3q_{00}^3 - 2q_{11}^4 + 2q_{00}^4 + q_{11}^5 - q_{00}^5 + 3q_{00}q_{11}^2 - 3q_{00}^2 q_{11} + 4q_{00}^3 q_{11} - 4q_{00}q_{11}^3 - 2q_{00}^3 q_{11}^2 + 2q_{00}^2 q_{11}^3 - 3q_{00}^4 q_{11} + 3q_{00}q_{11}^4)/12$

По мере увеличения длины ДВП объем расчетов значительно увеличивается. Однако исследование поведения формул таблицы путем численных расчетов показывает, что указанные ряды должны сходиться. Предел их схождения можно установить по фундаментальной теореме о регулярных марковских цепях [3], в соответствии с которой вектор вероятности стационарного состояния $\overline{q} = \{q_0, q_1\}$, где q_0, q_1 – стационарные вероятности появления нуля и единицы, определяется из матричного уравнения

$$\overline{q} \cdot P = \overline{q} \tag{4}$$

при соблюдении условия (1).

Подставляя (1) и (2) в (4), получаем

$$\begin{aligned} q_0 &= (1 - q_{11})/(2 - q_{11} - q_{00}), \\ q_1 &= (1 - q_{00})/(2 - q_{11} - q_{00}). \end{aligned} \tag{5}$$

Нетрудно видеть, что математическое ожидание ДВП совпадает со стационарной вероятностью появления единицы:

$$E\beta = q_1, \tag{6}$$

где q_1 определено в (5). Из выражения (6) можно оценить значения математического ожидания и дисперсии (3) выходной ДВП по параметрам генератора.

Нормированная автокорреляционная функция (АКФ), по определению, находится из соотношения

$$K(\tau) = (E(\beta_k \beta_{k+\tau}) - (E\beta)^2)/D\beta, \tag{7}$$

где β_k – k-е значение ДВП β, τ – смещение, $D\beta$ определяется по (3).

На рис. 3 показаны значения АКФ (7) выходных ДВП β для разных значений q_{00} и q_{11}. По оси абсцисс отложено τ.

Можно отметить следующее.

1 Излом АКФ при нулевом смещении свидетельствует о недифференцируемости выходной ДВП.

2 Если выполняется соотношение $q_{11} > 1 - q_{00}$, то выходная ДВП оказывается положительно коррелированной, причем корреляция оказывается тем больше, чем меньше q_{11}. Методом наименьших квадратов в этом случае получено хорошее совпадение АКФ с экспоненциальной функцией.

3 При $q_{00} = 1 - q_{11}$ выходная ДВП оказывается полностью некоррелированной.

4 При $q_{11} < 1 - q_{00}$ по мере увеличения смещения АКФ приобретает характер колебаний с убывающей амплитудой, причем затухание колебаний оказывается тем меньше, чем меньше q_{11}.

5 АКФ для симметричных значений q_{00} и q_{11} оказываются одинаковыми. Значения математических ожиданий при этом дают в сумме 1. Это свидетельствует об инверсии полученных в двух случаях ДВП, характер же их колебаний не изменяется.

Таким образом, варьируя параметры q_{00} и q_{11} можно синтезировать широкий класс недифференцируемых ДВП с заданными математическим ожиданием и автокорреляционной функцией.

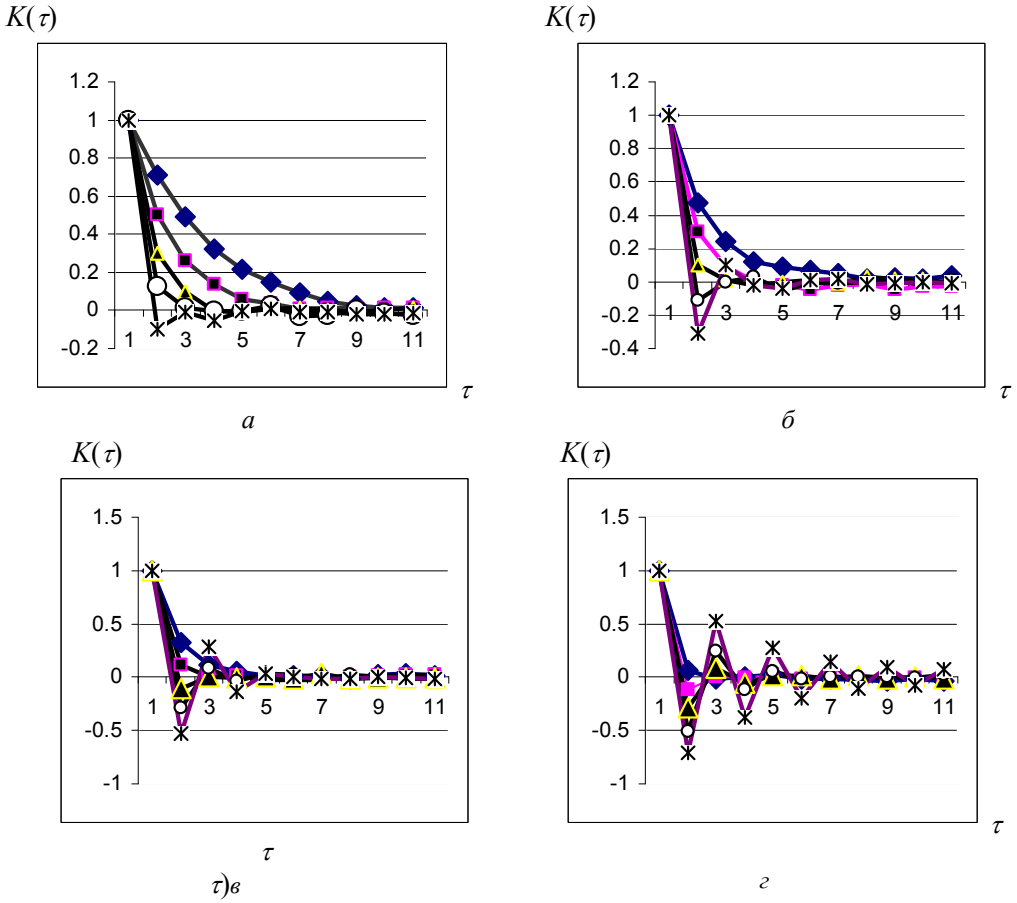


Рисунок 3 – АКФ выходных ДВП: *а* - q_{00} = 0,8, *б* - q_{00} = 0,6, *в* - q_{00} = 0,4, *г* - q_{00} = 0,2; ромб - q_{11} = 0,9, квадрат - q_{11} = 0,7, треугольник - q_{11} = 0,5, кольцо - q_{11} = 0,3, звездочка - q_{11} = 0,1

Интервал корреляции для монотонно убывающих АКФ можно оценить, приняв во внимание, что он должен быть близким к средней продолжительности цепочек из нулей n_0 и единиц n_1. Нетрудно видеть, что n_0 и n_1 для цепи Маркова (2) определяются последовательным количеством переходов 0→0 и 1→1 , то есть находятся из соотношения

$$q_{00}^{\,n_0} > 0{,}5, \qquad q_{11}^{\,n_1} > 0{,}5. \tag{9}$$

Выбрав по качественным критериям АКФ, определяем из (9) область допустимых значений параметров q_{00} и q_{11}. Пользуясь (7), можно эту область сузить до получения приемлемых выходных ДВП.

Полученные результаты найдут применение в анализе вероятностных характеристик и параметров сетей цифровой связи, используемых в банковской системе Украины.

Литература: ***1.*** *Протоколы и методы управления в сетях передачи данных— М.: Радио и связь, 1985. — 489 с.-С. 8-14.* ***2.*** *Д.. Кнут. Искусство программирования для ЭВМ.- Т. 2. - Получисленные алгоритмы. – М.: Мир. – 1977 – 482 с.* ***3.*** *Д. Тернер. Вероятность, статистика и исследование операций.//Пер. с англ.- М.: Статистика, 1976.– 432с. – С. 293-300.*