УСТРОЙСТВО ФОРМИРОВАНИЯ НЕБИНАРНОЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА БАЗЕ ПЛИС

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Карпович П.И.

Чердынцев В.А. – д-р техн. наук, профессор

В настоящее время большую популярность получили радиотехнические системы с расширением спектра, такие системы требуют наличия в системе источника случайных чисел. Ниже описано устройство формирования высококачественной не бинарной псевдослучайной последовательности (ПСП) по алгоритму «Вихрь Мерсенна».

В настоящее время наибольшее распространение получили следующие методы формирования небинарных ПСП: линейный конгруэнтный генератор, метод Фибоначчи с запаздыванием, регистр сдвига с линейной обратной связью, регистр сдвига с обобщенной обратной связью.

Наиболее новым методом является «вихрь» Мерсенна, он позволяет формировать не бинарные высококачественные ПСП с большим периодом и хорошими статистическим характеристиками без использования операции умножения, что позволяет экономить ресурсы вычислительных систем. Классический «вихрь» Мерсенна имеет период $2^{19937}-1$, что более чем достаточно для большинства практических приложений. Так же он имеет равномерное распределение k-распределение для бит v=1, 2,...32 - это позволяет порождать новые высококачественные ПСП отбрасывая любое, меньшее 32, количество младших бит. [1]

Рассмотрим алгоритм «вихря» Мерсенна для формирования w-размерных векторов над полем $F_2 = \{0,1\}$. Рекуррентное соотношение:

$$x_{k+n} = x_{k+m} \wedge \left(x_k^u | x_{k+1}^l\right) \cdot A, \tag{1}$$

где n — целое число, обозначает степень рекуррентности,
m — целое число, 1 < m < n,
A — матрица размером w x w с элементами поля F_2,
x_k^u - старшие w-r бит k-го слова,
x_{k+1}^l - младшие r бит k+1-го слова.

Для того чтобы избавится операции умножения в рекуррентном соотношении (1) матрицу A выберем вида

$$A = \begin{pmatrix} 0 & 1 & & & & \\ 0 & 0 & 1 & & & \\ 0 & \cdots & \cdots & \ddots & & \\ & & & & \ddots & \\ & & & & & 1 \\ a_{w-1} & a_{w-2} & \cdots & \cdots & \cdots & a_0 \end{pmatrix} \tag{2}$$

В случаи матрицы A вида (2), операцию умножения в рекуррентном соотношении (1) можно заменить следующим алгоритмом

$$xA = \begin{cases} x \gg 1, & x_0 = 0 \\ (x \gg 1) \wedge a, & x_0 = 1 \end{cases} \tag{3}$$

Для улучшения характеристик k-распределения по v-бит «вихрь» Мерсенна требует применения алгоритма закалки к выходным данным. Алгоритм закалки описан в [2].

На рисунке 1 изображена автокорреляционная функция в логарифмическом масштабе последовательности длинной 1 миллион выборок сформированной при помощи «вихря» Мерсенна. На рисунке 2 представлен амплитудный спектр данной последовательности, на рисунке 3 — гистограмма распределения данной псевдослучайной величины.

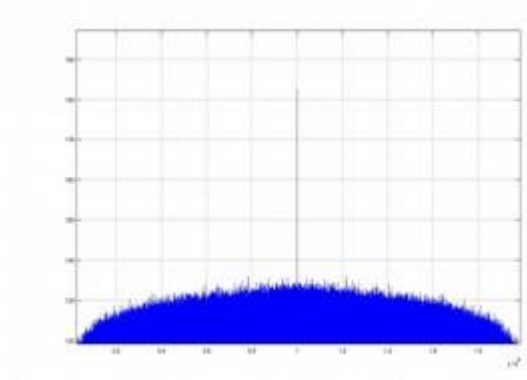

Рис. 1. – Автокорреляционная функция

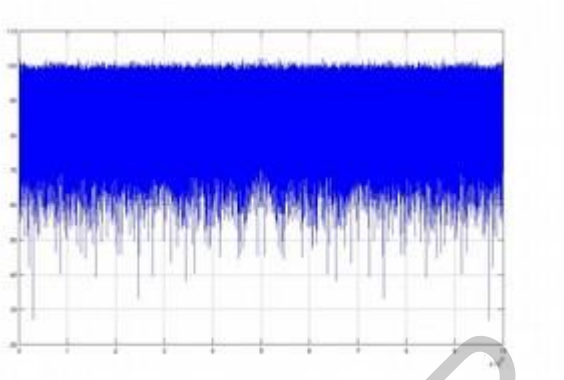

Рис. 2. – Амплитудный спектр

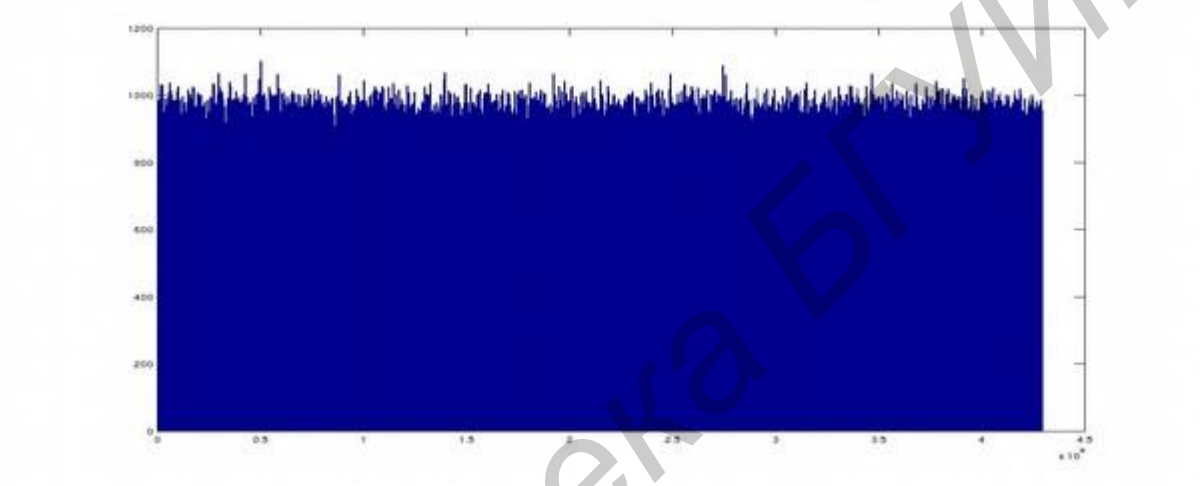

Рис. 3. – Гистограмма распределения псевдослучайной величины

Как видно из рисунков алгоритм «вихрь» Мерсенна способен формировать высококачественную псевдослучайную последовательность с равномерным законом распределения.

Список использованных источников:

1. Электронный ресурс. Режим доступа: http://www.math.sci.hiroshima-u.ac.jp