ФОРМИРОВАНИЕ РАВНОМЕРНО РАСПРЕДЕЛЕННОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ОТ ИСТОЧНИКА ПРОИЗВОЛЬНОГО ЗАКОНА РАСПРЕДЕЛЕНИЯ

Бахтин Александр Александрович
К.т.н., НИУ МИЭТ (г. Москва)
bah@miet.ru
Шарамок Александр Владимирович
К.т.н., доцент, НИУ МИЭТ (г. Москва)
sharamok@mail.ru

Аннотация. В статье приводятся уточнения ранее полученных результатов по теоретическому обоснованию формирования равномерно распределенных выходных последовательностей от источников случайных величин произвольного закона распределения. Показано, что вид закона распределения исходной случайной величины не имеет значения, важной является только информация о ширине носителя характеристической функции случайной величины.

Ключевые слова: датчик случайных чисел, равномерный закон распределения, характеристическая функция.

GENERATION OF UNIFORMLY DISTRIBUTED RANDOM NUMBERS FROM A SOURCE OF RANDOM NUMBERS WITH ARBITRARY DISTRIBUTION

A. Bakhtin
A. Sharamok

Summary. The article presents refinements of previously obtained results on uniformly distributed number generation from sources of random numbers with an arbitrary distribution. It is shown that a type of a distribution of initial random numbers does not matter, only the information about the width of a characteristic function carrier of is important.

Keywords: random numbers generator, uniform distribution of random numbers, characteristic function.

Введение

Трудно переоценить важность формирования случайных чисел с точки зрения практического построения систем и средств телекоммуникаций, вычислительных средств и средств криптографической защиты информации. Случайные числа необходимы и используются при построении экспериментов, решении вычислительных алгоритмов недетерминированными методами, моделировании работы телекоммуникационных систем и устройств [1]. При необходимости реализации физических датчиков случайных числе в конкретных технических средствах эта задача, как правило, является не тривиальной и требует решения комплекса математических и технических подзадач.

Зачастую к последовательности случайных чисел предъявляется требование равномерности ее закона распределения. Указанное требования является достаточно сложным, с точки зрения практической реализации, так как в составе и окружении разрабатываемых средств имеется широкий набор источников случайных величин, характеристики которых, прежде всего, не соответствуют требованию равномерности закона распределения случайной величины. В настоящей статье авторы приводят уточнение ранее полученных теоретических результатов приведения значений случайной величины с произвольным законом распределения к закону с равномерным распределением [2].

Процесс измерения случайной величины

Пусть ζ наблюдаемая случайная величина, имеющая плотность распределения $P_\zeta(t)$. Процесс измерения ζ условно описан на рис. 1.

С математической точки зрения процесс измерения величины ζ с n значными (верными) битами означает, что ошибка измерения не превосходит половины цены последней сохраненной цифры [3].

$\hat{\zeta}$ — имеет n значных (верных) бит.

Заметим, что $\hat{\zeta}$ есть двоичный вектор $\zeta_n \ldots \zeta_s\zeta_{s-1} \ldots \zeta_1\zeta_0$. Рассмотрим S младших бит $\zeta_{s-1} \ldots \zeta_1\zeta_0$. Разобьем интервал измерения наблюдаемой случайной величины ζ на подинтервалы длины h.

Введем в рассмотрение случайную величину ξ, определяемую условием $\xi \equiv \zeta \pmod h$.

Охарактеризуем эту случайную величину:

- случайная величина ξ изменяется в пределах $0 \leq \xi < h$;

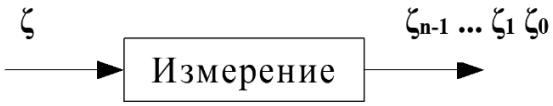

Рис. 1. Процесс измерения случайной величины

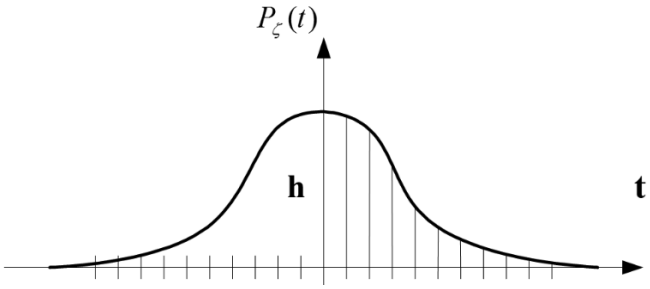

Рис. 2. Разбиение носителя $P_\zeta(t)$ на равные интервалы

- всякое значение случайной величины ξ связано с некоторым значением случайной величины ζ равенством $\zeta = kh + \xi$, где k — некоторое целое число.

Функция плотности вероятности вновь введённой случайной величины

Согласно данному выше определению, функция плотности вероятности $P\xi(t)$ случайной величины ξ имеет вид:

$$P_\xi(t) = \sum_{k\in Z} P_\zeta(t+kh), \quad 0 \le t < h. \tag{1}$$

Пусть $\hat{P}_\zeta(\omega)$ — характеристическая функция случайной величины ζ. Согласно формуле суммирования Пуассона [4] имеет место:

$$h\sum_{k=-\infty}^{k=+\infty} P_\zeta(t+kh) = \sum_{k=-\infty}^{+\infty} \hat{P}_\zeta\left(\frac{2\pi k}{h}\right) e^{\frac{i2\pi kt}{h}}. \tag{2}$$

или, между функцией плотности случайной величины ξ и характеристической функцией $\hat{P}_\zeta(\omega)$ имеет место связь:

$$P_\xi(t) = \sum_{k\in Z} \frac{1}{h}\hat{P}_\zeta\left(\frac{2\pi k}{h}\right) e^{\frac{i2\pi kt}{h}}. \tag{3}$$

Разложим сумму в правой части равенства (3) на две составляющие:

$$P_\xi(t) = \frac{1}{h}\hat{P}_\zeta(0) + \frac{1}{h}\sum_{k=-\infty}^{+\infty|} \hat{P}_\zeta\left(\frac{2\pi k}{h}\right) e^{\frac{i2\pi kt}{h}}. \tag{4}$$

Пусть h выбираем так, что $\pi/h > \nu_0(\zeta)$, где $\nu_0(\zeta)$ частота, за пределами которой характеристическая функция $\hat{P}_\zeta(\omega)$ имеет пренебрежимо малое абсолютное значение. Последнее означает величина π/h не менее частоты Найквиста сигнала $P_\zeta(t)$.

В этих предположениях формула (4) принимает вид:

$$P_\xi(t) \overset{\bullet}{=} \frac{1}{h}\hat{P}_\zeta(0), \quad но \quad \hat{P}_\zeta(0) = \int_{-\infty}^{+\infty} P_\zeta(t)dt = 1. \tag{5}$$

Следовательно, $P_\xi(t) = 1/h \; при \; 0 \le t < h$, то есть ξ равномерно распределенная величина, при условии, что $\hat{P}_\zeta(0) \ne 0$ и характеристическая функция случайной величины ζ быстро стремится к нулю, при ω стремящемся к бесконечности.

Практические требования к приведению плотности вероятности к равномерному виду

Сформулируем в следующем виде практические требования к приведению плотности вероятности $P\xi(t)$ величины ξ к равномерному виду:

1. Спектр функции $P\zeta(t)$ должен быть конечным, т.е. $\hat{P}_\zeta(\omega) \ne 0$ при $-\nu_0(P_\zeta) < \omega < +\nu_0(P_\zeta)$, и стремиться к нулю вне этого интервала, где $\nu_0(P_\zeta)$ — частота Найквиста.
2. Ряд, образующий функцию Pξ(t), сходится абсолютно и равномерно.

Пусть при этом:

$$\sum_{k=-\infty}^{-N-1}\left|\hat{P}_\zeta(t+kh)\right| + \sum_{k=N+1}^{+\infty}\left|\hat{P}_\zeta(t+kh)\right| < \sigma. \tag{6}$$

Тогда при $\pi/h > \nu_0$ или $h < \pi/\nu_0$ имеет место:

$$\sum_{k=-N}^{+N} \hat{P}_\zeta(t+kh)h \approx \hat{P}_\zeta(0) + \sigma, \quad \hat{P}_\zeta(0) \ne 0. \tag{7}$$

Т.е. функция $P\xi(t)$ представляет собой функцию плотности равномерного распределения, с ошибкой порядка $\sigma/2N$.

Эта модель точная, если характеристическая функция распределения $P_\zeta(t)$ имеет конечный носитель (т.е. спектр функции $P_\zeta(t)$ сосредоточен на отрезке $[-\nu_0,+\nu_0]$). В противном случае модель приближенная, и степень приближения зависит от выбора шага дискретизации h.

Рассмотренная выше модель справедлива для идеальной величины, на практике измеряемая величина ζ является суммой идеальной величины ζ_0 и шума ε (статистически независимого от ζ_0), $\zeta = \zeta_0 + \varepsilon$.

Пусть идеальная величина ζ_0 имеет частоту Найквиста $\nu_0 = \nu(P\zeta_0)$, ошибка ε имеет частоту Найквиста $\nu_1 = \nu(P_\varepsilon)$. Обозначим ν* = max$(\nu(P\zeta_0), \nu(P_\varepsilon))$. Базовые ограничения на выбор шага дискретизации имеют следующий вид:

$$\pi / h > \nu^* \Leftrightarrow h < \pi / \nu^*. \quad (8)$$

Пусть:

- $d > 0$ минимальный дискрет измерения «наблюдаемой» случайной величины ζ;
- прибор измерения гарантирует значимость $[-\log_2 d]$ бит [3].

Для формирования равномерно распределенной случайной величины должно выполняться условие $d < h < \pi / \nu^*$. Величины h и d связаны равенством $h = k \cdot d$ $(k > 1)$. $k = 2^s$ и пусть $d = 2^{-n}$, тогда $h = 2^s \cdot 2^{-n} = 2^{-(n-s)}$.

Выводы

На основании приведенных выше рассуждений делаются следующие выводы:

- для формирования равномерно распределенной случайной величины ξ по результатам измерения наблюдаемой случайной величины ζ форма ее функции плотности распределения несущественна, существенную роль играет информация о полосе частот, в которой сосредоточена характеристическая функция функции $P_\zeta(t)$;
- если случайная величина ζ представляет собой смесь двух статистически независимых случайных величин ζ_0 и ε, из которых ε — случайный шум, то рассматриваемая модель может использоваться для формирования почти равномерно распределенной случайной величины ξ, если выполняется условие: носитель характеристической функции плотности вероятности шума уже носителя характеристической функции плотности вероятности случайной величины ζ_0 и при этом выполняется условие $\pi / h > \nu_0(\zeta_0)$.

Изложенные выше положения позволяют разрабатывать датчики случайных чисел в составе широкого круга аппаратуры, не имеющей специальных источников физического шума. Применяя изложенную модель, можно теоретически обосновать свойства датчиков, построенных, например, на основе клавиатурной работы оператора, времени выхода абонента на связь и т.д.

Дополнительно авторы отмечают, что на разработку приведенных результатов огромное влияние оказал научный руководитель одного из авторов Амербаев В. М.

ЛИТЕРАТУРА

1. Kelton D., Law A., Simulation Modelling and Analysis Paperback, Edition 3, illustrated, New York City, USA, McGraw-Hill, 2000.
2. Шарамок А. В., Методы повышения защищенности УКВ радиосредств и разработка системы защиты информации телекоммуникационного комплекса: Москва, Науч.-произв. центр «СПУРТ», дис. ктн, 2004 г., 124 стр.
3. Новицкий П. Ф., Зограф И. Д. Оценка погрешностей средств измерения, Л., Энергоатомиздат, 1985.
4. Titchmarsh E. C., Introduction to the theory of Fourier's integral, Oxford University Press, 1937.

Журнал «Современная наука: актуальные проблемы теории и практики»