Метод построения хаотических бинарных кодов

С.В. Савельев, Л.А. Морозова

Фрязинский филиал Федерального государственного бюджетного учреждения науки Института радиотехники и электроники им. В.А. Котельникова российской академии наук; Фрязино, пл. Введенского, 1; e-mail: savelyev@ms.ire.rssi.ru.

Предложен метод построения счетного множества бинарных ортогональных хаотических последовательностей с большим информационным объемом. Метод основан на использовании свойств радиофизической системы с динамическим хаосом.

The method of construction of a countable set of binary orthogonal chaotic sequences with a large information volume. The method is based on the properties of radio systems with dynamic chaos.

Развитие современных телекоммуникационных средств с большой скоростью передачи информации основано на использовании широкополосных сигналов с большой информационной емкостью [1 - 3]. В результате расширения спектра частот несущего сигнала возможно увеличение скорости передачи информации, повышение устойчивости и надежности систем связи при наличии различных возмущений. Использование широкополосных сигналов обеспечивает высокую пропускную способность каналов связи, позволяет ослабить вредное влияние помех и выделять полезный сигнал при соотношении сигнал / шум много меньше единицы. Первоочередным достоинством широкополосных хаотических систем является высокая скрытность и электромагнитная совместимость с другими беспроводными средствами связи за счет применения шумоподобных сигналов со сверхнизкой спектральной плотностью. Такие широкополосные сигналы могут использоваться для связи в многоканальных и многоадресных системах с кодовым разделением абонентов CDMA (Code Division Multiple Access System), и в беспроводных системах связи с расширением спектра WSSC (Wireless Spread Spectrum Communication Systems), что обеспечивает высокие требования, предъявляемые по защите передаваемой информации от несанкционированного доступа.

Глобальное распространение индивидуальных средств связи совместно с условиями обеспечения помехоустойчивости и скрытности диктуют повышенные требования на разработку новых принципов формирования семейств кодирующих сигналов с большим объемом. Частичное решение проблемы представлялось в переходе от традиционных систем связи с частотно-временным разделением абонентов к системам с кодированием широкополосными псевдослучайными сигналами, когда каждый из абонентов обязан использовать индивидуальный код или свою кодовую последовательность. Однако стремительное развитие многопользовательских персональных связных систем стимулирует поиск новых подходов к разработке семейств кодовых последовательностей с большой информационной емкостью. Перспективными здесь являются класс сигналов с расширением спектра на основе хаотических сигналов [3].

При создании систем с кодовым разделением абонентов решающим является математический алгоритм, порождающий ансамбль кодовых последовательностей. Наиболее значимым для создания непериодической случайной последовательности является такой алгоритм, который позволяет кодирование каждого бита передаваемой информации с помощью своего неповторяющегося во времени набора символов. Такой случай может быть реализован при использовании явления динамического хаоса.

В работе представлена методика построения множества бинарных ортогональных хаотических последовательностей, основанная на использовании реализации хаотического процесса, построения на его основе базовой хаотической бинарной последовательности и создании семейства бинарных ортогональных последовательностей путем введения последовательного временного сдвига в базовую последовательность для каждой бинарной последовательности из порождаемого множества.

Пусть известна временная реализация *F(t)* действительно хаотического процесса, порождаемого детерминированной динамикой нелинейной системы. При этом автокорреляционная функция процесса *F(t)* убывает до нуля на некотором промежутке времени, что является следствием перемешивания. Это значит, что система теряет взаимосвязь между состояниями с достаточно большим промежутком времени. Рассмотрим одну из возможностей генерации хаотической бинарной последовательности, используя временную реализацию такого хаотического процесса. Построение бинарной хаотической последовательности в простейшем ассиметричном случае можно представить как:

$$B_k = \frac{1}{2}\{1 + sign[F'(t_k)]\} \qquad (1)$$

где производная хаотической функции *F(t)* вычисляется в моменты времени t_k с шагом не более величины обратной верхней граничной частоты хаотического процесса. Хаотическая последовательность двоичных символов от хаотической порождающей функции имеет место, когда моменты времени, в которые производится отчет первой производной, связаны рекуррентным соотношением:

$$\frac{2\pi}{\omega_d} = \int_{t_k}^{t_{k+1}} \{1 + [F'(t)]^2\} dt \qquad (2)$$

где ω_d - наибольшая значимая частота функции *F(t).*

В (2) интеграл вычисляется по кривой временной реализации функции *F(t)* при движении изображающей точки с единичной скоростью. Плотная выборка значений производной хаотической функции гарантирует хаотичность порождаемой предложенным алгоритмом квазибинарной последовательности $B_k^{/}$.

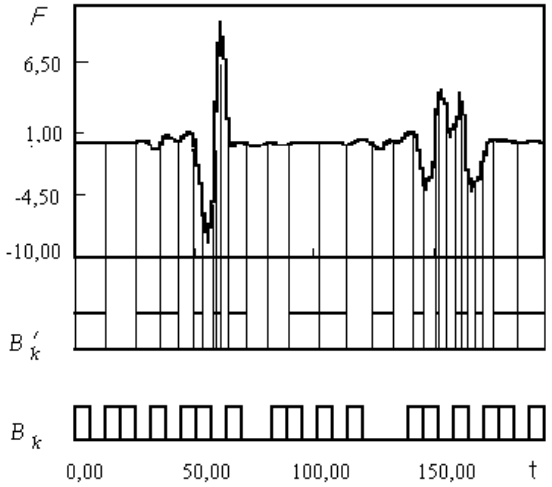

Рис. 1.

На рис.1 схематически представлен процесс генерации квазибинарной хаотической последовательности $B_k^{/}$ в соответствии с предложенным математическим алгоритмом. Внизу рисунка представлена «исправленная» последовательность B_k после обработки ее специализированным процессором, представляющая собой искомую действительно

хаотическую бинарную последовательность, которая будет являться базовой для создания семейства ортогональных бинарных хаотических последовательностей. На реальную хаотичность генерируемой бинарной последовательности указывает порождающий алгоритм, определенный равенствами (1) и (2), такой, что для всех k справедливо соотношение:

$$\frac{2\pi}{\omega_d} \geq t_{k+1} - t_k \tag{3}$$

означающее, что длительность каждого символа генерируемой бинарной последовательности $B_k^{/}$ не превышает временного интервала дискретизации для определения $F(t)$. Таким образом, исходя из хаотичности порождающей функции $F(t)$, неравенство (3) является необходимым и достаточным условием хаотичности формируемой бинарной последовательности B_k в соответствии с теоремой Шеннона [1].

Реализация предлагаемого метода основана на статистических свойствах локально неустойчивых систем, когда функция автокорреляции от хаотической функции спадает до нуля за время предсказуемости, по порядку величины равное характерному времени обхода странного аттрактора системы с динамическим хаосом [3]. Проследим изменение функции автокорреляции хаотической бинарной последовательности, реализованной в соответствии с предложенным методом, в случае реальной порождающей хаотической функции $F(t)$.

Пусть $F(t)$ есть решение уравнений, описывающих динамику системы с выделенной инерционностью [4]. Динамика системы с выделенной инерционностью характеризуется большим разнообразием колебательных процессов, включающих как регулярные, так и хаотические колебательные режимы с различной степенью автокорреляции. Тогда, следуя [10], пусть порождающая хаотическая функция $F(t)$ будет определяться четырехпараметрической системой нелинейных дифференциальных уравнений:

$$\begin{aligned}
&\dot{F} = G + (m_1 - m_2)F - FZ,\ F \leq q \\
&\dot{F} = G - m_2 F - qF,\ F > q \\
&\dot{G} = -F \\
&\dot{Z} = -gZ + gI(2F - m_2 J)(2F - m_2 J)^2,\ I(y) = \begin{cases} 1,\ y \geq 0 \\ 0,\ y < 0 \end{cases} \\
&\dot{J} = F - m_2 J
\end{aligned} \tag{4}$$

первые три уравнения описывают безинерционный колебательный процесс, где динамическая характеристика нелинейного активного элемента имеет линейный участок и участок с насыщением, четвертое и пятое уравнение отражают действие однополупериодного инерционного преобразователя на крутизну динамической характеристики в зависимости от выходного сигнала активного элемента. Обозначения переменных такие же, как в [4]. Развитый хаотический режим в системе (4) имеет место при m_1 = 1,8, m_2 = 0,3, q = 0,5, g = 0,01. Движение изображающей точки в фазовом пространстве системы представляет странный аттрактор в окрестности петли седло-фокус. Корреляционная функция экспоненциально убывает с декрементом, определяемым энтропией Колмогорова.

Для построения базовой хаотической бинарной последовательности использовалась временная реализация $F(t)$, когда дифференциальный закон распределения плотности вероятности колебаний близок нормальному Гауссову. Метод построения множества бинарных ортогональных хаотических последовательностей на

основе базовой последовательности тесно связан с эволюцией автокорреляционной функции (АКФ):

$$R(t;t+T)=\langle B_k(t)B_k(t+T)\rangle-\langle B_k(t)\rangle\langle B_k(t+T)\rangle \qquad (5)$$

где угловые скобки $\langle ...\rangle$ означают усреднение по ансамблю реализаций процесса $B_k(t)$. Исключая переходной процесс, хаотические колебания являются процессом стационарным и эргодическим. Это означает, что усреднение по ансамблю можно заменить усреднением по времени вдоль одной типичной реализации. АКФ, которая нормируется на максимальное значение при T = 0. Поведение $R(t,t+T)$ позволяет найти значение величины временной задержки T, приводящей к потере связи с предысторией для бинарной хаотической последовательности $B_k.(t)$.

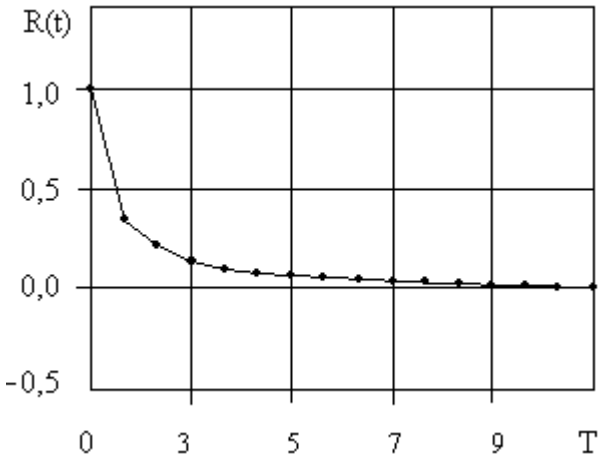

Рис. 2.

На рис. 2 представлена нормированная АКФ бинарной функции B_k. Хаотичность функции подтверждается экспоненциальным убыванием корреляций. Численный анализ показывает уменьшение автокорреляционной функции до нуля уже при значениях T = $10T_1$, где T_1 - длительность одного символа бинарной последовательности, что по порядку величины соответствует характерному периоду колебаний $F(t)$. Выявленное свойство АКФ $R(t,T)$ позволяет формировать счетное множество бинарных ортогональных хаотических последовательностей B_k^N путем введения в базовую последовательность B_k временной задержки равной $10T_1N$, где N=1,2,…. Хаотичность и ортогональность формируемого семейства бинарных последовательностей совместно с быстродействующими цифровыми процессорами в системах связи позволит на практике осуществить кодовое разделение большого числа пользователей. Простые расчеты показывают, что при центральной частоте передатчика 1Ггц и реальной временной задержке не более 1 секунды система с предложенным алгоритмом обеспечивает одновременное кодовое разделение 100000 абонентов.

Численные расчеты АКФ подтверждают значимость предложенного метода формирования счетного множества бинарных ортогональных хаотических последовательностей на основе базовой последовательности, полученной методами нелинейной динамики, путем последовательного введения относительной задержки с кратностью нескольких длительностей единичного бинарного символа. Свойство взаимной ортогональности и хаотичности множества бинарных последовательностей позволяет использовать их для передачи информации с кодовым разделением абонентов в системах с повышенной защитой. Предложенный метод построения счетного множества бинарных ортогональных хаотических последовательностей

реально осуществим в широком диапазоне длин волн в качестве семейства хаотических кодов с большим информационным объемом.

Работа выполнена при поддержке РФФИ, грант № 16-07-00956.

Литература

1. Shannon C.E., A Mathematical Theory of Communication, Bell System Techn. J., 1948. V. 27, N 3, P. 379.
2. Котельников В.А. Теория потенциальной помехоустойчивости. // М.: Радио и связь, 1998.
3. Ю.В. Гуляев, В.Я. Кислов, В.В. Кислов. Новый класс сигналов для передачи информации – широкополосные хаотические сигналы // ДАН. 1998. Т.359. № 6. С.750-754.
4. С.В.Савельев. Математическая модель мощного усилительного каскада на биполярном транзисторе. Журнал радиоэлектроники [электронный журнал]. 2017. №6. Режим доступа: http://jre.cplire.ru/jre/jun17/10/text.pdf