Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Об одном биологическом генераторе псевдослучайных чисел

Цыпышев Вадим Николаевич,
к.ф.-м.н., ведущий инженер, С-Терра СиЭсПи

Цели и методы

- Цель настоящего доклада состоит в том, чтобы предложить метод построения биологических датчиков случайных чисел, надежно обосновываемых в рамках общей теории хаотических процессов

О хаотических процессах

- Королев В.Ю.
- Вероятностно-статистический анализ хаотических процессов с помощью смешанных гауссовских моделей. Декомпозиция волатильности финансовых индексов и турбулентной плазмы //
- М.: МГУ, 2008. — 390 с.

Результаты монографии

- В качестве “элементарных” математических моделей динамики на очень малых временных масштабах рассматриваются обобщенные дважды стохастические пуассоновские процессы (обобщенные процессы Кокса) со скачками, имеющими конечную дисперсию.
- В соответствии с принципом максимальной энтропии такие процессы являются наилучшими моделями неоднородных хаотических потоков.

Результаты монографии

- Асимптотический подход, основанный на предельных теоремах для обобщенных процессов Кокса как моделей неоднородных хаотических случайных блужданий приводит к макромоделям стохастических хаотических процессов типа подчиненных винеровских процессов (процессов броуновского движения со случайными и зависящими от времени коэффициентами сноса и диффузии).

Результаты монографии

- Аппроксимации для распределений (логарифмов) приращений процессов эволюции следует искать в виде общих сдвиг/масштабных смесей нормальных законов, в которых смешивающий закон определяется накопленной (интегральной) интенсивностью потоков соответствующих информативных событий (элементарных скачков, “тиков”).

Результаты монографии

- В самой общей постановке задача статистического оценивания смешивающего распределения является некорректной, так как общие сдвиг/масштабные смеси нормальных законов не являются идентифицируемыми

Результаты монографии

- В рамках общего принципа регуляризации некорректных задач, исходная задача заменяется задачей отыскания решения, наиболее близкого к истинному в классе конечных дискретных сдвиг/масштабных смесей нормальных законов. Эта “редуцированная” задача уже является корректной и имеет единственное решение, так как семейство конечных дискретных сдвиг/масштабных смесей нормальных законов идентифицируемо.

Применение результатов монографии в медицинской практике

- Т. В. Захарова, М. М. Подлесный, “Смеси нормальных законов в задаче поиска опорных точек по сигналу миограммы” //
- Системы и средства информ., 26:3 (2016), 106–121

- http://www.mathnet.ru/links/81388bf51b9204a63fd039365a3ae706/ssi478.pdf

Применение результатов монографии в медицинской практике

- Данная статья посвящена исследованию вероятностных характеристик миограммы, представляющей собой запись электрической активности мышц.
- Предлагается в качестве математической модели шума миограммы использовать конечные сдвиг-масштабные смеси нормальных законов.
- Задача разделения смесей решается с помощью стохастического EM (expectation–maximization) алгоритма, и полученные данные используются для нахождения точек привязки на основе CUSUM-статистик.

Применение результатов монографии в медицинской практике

- Одним из важнейших направлений современной медицины является изучение активности головного мозга и определение расположения его функциональных зон
- С этой целью используется м□гнитоэнцеф□логр□фия (МЭ□) в комбина□ции с магнито-резонансной томографией.
- В целях повышения уровня полезного сигнала пациент в ответ на внешний раздражитель выполняет одни и те же действия, которые регистрируются на МЭГ и миограмме
- В целях дальнейшего анализа выявляется вероятностное распределение приращений значений миограммы

Применение результатов монографии в медицинской практике

- Основной результат статьи состоит в том, что приращения миограммы является нестационарным случайным процессом
- Вероятностное распределение приращений миограммы находится в классе смесей двух нормальных распределений
- Таким образом, последовательность приращений миограммы является неоднородным хаотическим процессом случайных блужданий

Интерпретация результатов статьи

- Время, в течении которого увеличивается значение миограммы, также является неоднородным хаотическим процессом случайных блужданий
- Время, в течении которого увеличивается значение миограммы, совпадает со временем реакции индивида на повторяющийся раздражитель
- Следовательно, время реакции индивида на повторяющийся раздражитель является неоднородным хаотическим процессом случайных блужданий

Интерпретация результатов статьи

- Вероятностное распределение времени реакции индивида находится в классе смесей двух нормальных распределений

Парадигма построения БиоДСЧ

- Источником случайности является время реакции индивида на постоянно повторяющийся внешний раздражитель, состоящей в выполнении заранее предопределенных действий

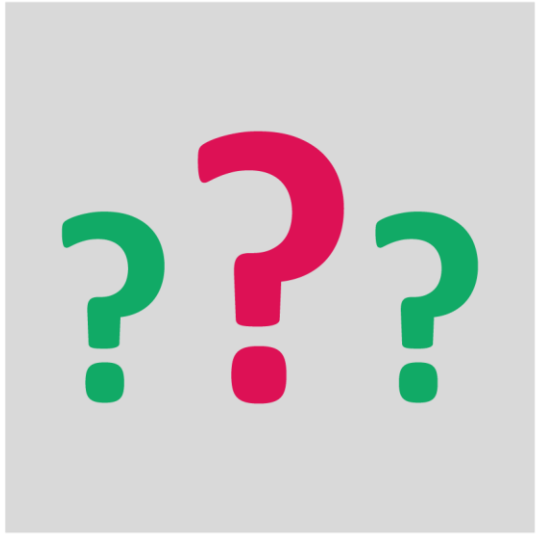
Проверка соответствия модели

- Проверка соответствия Биологического ДСЧ модели статьи [Захарова, Подлесный] состоит в построении вероятностного распределения, согласующегося с эмпирической функцией распределения, построеннойпо выборке из съемов с БиоДСЧ
- В случае, если такое распределение является смесью двух нормальных распределений, можно считать, что БиоДСЧ соответствует модели

Существование БиоДСЧ, реализующих предложенную парадигму построения

- БиоДСЧ, применяемый в продуктах С-Терра СИЭСПИ, умозрительно соотвествующий предложенной парадигме построения, соответствует модели
- Поскольку ранее состоятельность указанного БиоДСЧ была обоснована стандартными методами, можно считать, что предложенная парадигма построения БиоДСЧ реализуема на практике

Вопросы



Контактная информация

Электронная почта:

vcypyshev@s-terra.ru

Телефон:

+7 915 105 94 85

Facebook:

facebook.com/tsypyschev

Сайт:

www.s-terra.ru