ЦЕПИ МАРКОВА ВЫСОКОГО ПОРЯДКА: МАЛОПАРАМЕТРИЧЕСКИЕ МОДЕЛИ И ИХ ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКИЙ АНАЛИЗ

Харин Ю.С.

НИИ прикладных проблем математики и информатики Белгосуниверситета, пр. Независимости 4, 220030 Минск, Беларусь Kharin@bsu.by

Существующая теория вероятностно-статистического анализа временных рядов $x_t \in \mathbf{A}$, $t \in \mathbf{Z}$, в настоящее время глубоко развита для «непрерывных» моделей (гауссовские, регрессионные, трендовые, авторегрессионные, ARIMA и др.), у которых пространство состояний $\mathbf{A} \subseteq \mathbf{R}^m$ и имеет ненулевую меру Лебега $\mathrm{mes}(\mathbf{A}) > 0$. В связи с цифровизацией экономики и всей человеческой деятельности все чаще приходится использовать дискретные временные ряды (ДВР) [1], у которых $\mathbf{A} = \{0, 1, \ldots, N-1\}$ — дискретное множество мощности $N = |\mathbf{A}|$, $2 \le N \le +\infty$. ДВР широко применяются на практике: криптология и защита информации ($N = 2$); генетика ($N = 4$); экономика; персонализированная медицина.

Универсальная модель ДВР [2] — однородная цепь Маркова достаточно высокого порядка $s \in N$ на вероятностном пространстве $(\Omega, F, \mathbf{P})$:

$$\mathbf{P}\left\{x_t = j_t | F_{t-1}\right\} \equiv \mathbf{P}\left\{x_t = j_t | x_{t-1} = j_{t-1}, \ldots, x_{t-s} = j_{t-s}\right\} = p_{j_{t-s},\ldots,j_{t-1},j_t},$$

где s — глубина памяти, $\mathrm{P} = \left(p_{j_1,\ldots,j_s,j_{s+1}}\right)$ — $(s+1)$-мерная матрица вероятностей одношаговых переходов. К сожалению, вычислительная сложность оценивания этой модели по наблюдениям экспоненциально растет с ростом s: $O\left(N^{s+1}\right)$. Для преодоления этого «проклятия размерности» предлагается использовать так называемые малопараметрические (parsimonious) модели, для которых $\mathrm{P} = \mathrm{P}(a)$, $a = (a_1, \ldots, a_d) \in \mathbf{R}^d$, $d \ll N^{s+1}$.

Нами предложены три основных подхода к построению малопараметрических моделей. **Первый подход** состоит в сжатии множества различных значений элементов матрицы P:

$$p_{j_1,\ldots,j_s,j_{s+1}} = q_{B(j_1,\ldots,j_s),j_{s+1}},$$

где $B(\cdot)$: $\mathbf{A}^s \to \mathbf{A}^r$ — некоторая дискретная функция, $r < s$, Q — некоторая $(r+1)$-мерная стохастическая матрица. Примеры моделей ДВР, построенных этим подходом: цепь Маркова порядка s с r частичными связями, цепь Маркова условного порядка, цепь Маркова переменного порядка. **Второй подход** состоит в использовании порождающего уравнения:

$$p_{j_1,\ldots,j_{s+1}} = q_{j_{s+1}}\left(\theta(j_1, \ldots, j_s; a)\right), \quad j_1, \ldots, j_{s+1} \in \mathbf{A},$$

где $\{q_j(\theta) : j \in \mathbf{A}\}$ — некоторое стандартное дискретное распределение вероятностей на $\mathbf{A}$, зависящее от некоторого параметра θ. ДВР, построенные этим подходом: модель Джекобса — Льюиса, MTD-модель, DAR(s), BCNAR(s), BiCNAR(s), PCNAR(s). **Третий подход** использует искусственную нейронную сеть для репараметризации матрицы P.

В докладе представлены следующие результаты вероятностно-статистического анализа малопараметрических моделей:

1) критерий и достаточные условия эргодичности, свойства s-мерного стационарного распределения;

2) методы и алгоритмы статистического оценивания параметров модели $a \in \mathbf{R}^d$ по наблюдениям $x_1, \ldots, x_T$;

3) алгоритмы статистической проверки гипотез о параметрах a;

4) алгоритмы статистического прогнозирования ДВР;

5) методы робастного статистического анализа [3].

Теоретические результаты проиллюстрированы в компьютерных экспериментах на модельных и реальных данных.

Литература

1. Kharin Yu. *Robustness in Statistical Forecasting.* N.Y.: Springer, 2013.
2. Doob J. *Stochastic Processes.* N.Y.: Wiley, 1953.
3. Kharin Yu., Voloshko V. *Robust estimation for Binomial conditionally nonlinear autoregressive time series based on multivariate conditional frequencies* // Journal of Multivariate Analysis. 2021. Vol. 185. P. 11–27.

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Харин Ю.С., Мальцев М.В., Гайдук А.Н., Орлов А.А., Палуха В.Ю., Сергеев А.И.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь kharin@bsu.by, maltsew@bsu.com, gaidukan@bsu.com, alex.orlov.official@gmail.com, palukha@bsu.by, giftis95@mail.ru

Информационные технологии стали неотъемлемой частью современного общества. Информация является важнейшим ресурсом, нуждающемся в надежной защите, поэтому специалисты по защите информации требуются каждой компании, заинтересованной в конфиденциальности, целостности и сохранности своих данных. Потребность в таких кадрах обуславливает необходимость качественной подготовки студентов высших учебных заведений по специальностям, связанным с защитой информации. В Белорусском государственном университете ведется подготовка по специальностям 1-98 01 01-01 «Компьютерная безопасность (направление — математические методы и программные системы)», 1-98 01 01-02 «Компьютерная безопасность (направление — радиофизические методы и программно-технические средства)» и 1-97 01 02 «Прикладная криптография». С 2000 года в номенклатуру специальностей научных работников Республики Беларусь включена специальность 05.13.19 «Методы и системы защиты информации. Информационная безопасность». Таким образом, разработка и совершенствование учебных материалов для подготовки специалистов в области защиты информации является актуальной задачей. В 2001 году в Научно исследовательском центре прикладных проблем математики и информатики (в настоящее время — НИИ прикладных проблем математики и информатики) был разработан компьютерный практикум по математическим методам защиты информации [1], предназначенный для практических занятий студентов. С момента выхода практикума появились новые криптографические алгоритмы и протоколы, знание которых необходимо современному квалифицированному IT-специалисту. Кроме того, опыт работы преподавателей специализированных дисциплин показал, что необходимо внести изменения и дополнения в организацию и наполнение практикума.

Разработанный практикум дополняет изданный в Белорусском государственном университете учебник «Криптология» [2] и состоит из следующих составных частей: теоретический материал, задания для лабораторных занятий, выполняемых на компьютере, программная оболочка. Практикум включает в себя такие разделы криптологии, как простейшие («ручные») криптосистемы; генерация и тестирование псевдослучайных последовательностей; алгоритмы шифрования, хэширования, выработки и проверки электронной цифровой подписи; криптографические протоколы. Программная оболочка практикума предназначена для изучения и исследования учащимися криптографических алгоритмов, а также для выполнения заданий практикума. Реализована созможность воздавать криптографические алгоритмы из составных частей (блоки подстановок, перестановок, сумматоры и др.). Программа оснащена удобным интерфейсом, а также имеет архитектуру, позволяющую быстро добавлять новый функционал. Интерфейс программной оболочки практикума представлен на рисунке 1 (реализована сеть Фейстеля).