Math-Net.Ru

Общероссийский математический портал

А. М. Зубков, Рецензия на книгу Goldreich Oded. “Modern Cryptography, Probabilistic Proofs and Pseudorandomness”, *Теория вероятн. и ее примен.*, 1999, том 44, выпуск 3, 687–690

DOI: <https://doi.org/10.4213/tvp816>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.6.47.48

26 апреля 2023 г., 13:39:38

таты снабжены ссылками, а отсутствие ссылки означает, что ранее этот факт в литературе не обсуждался. Поскольку большая часть приводимых результатов принадлежит самим авторам, читателю ввиду отсутствия ссылки подчас трудно понять, кто из них и когда установил тот или иной результат. В книге явно не хватает историко-библиографических замечаний в конце текста. Такие замечания, снабженные дополнительной современной библиографией, несомненно, пошли бы на пользу читателю.

Спорной представляется мне и идея поместить классические монографии Андерсона, Лемана, Гаека и Шидака, Хеннана и т.д. в списке литературы дважды: в русской и английской части. На мой взгляд, это создает определенную путаницу и не дает никаких преимуществ. Впрочем, эти недостатки легко устранить при последующих изданиях.

Монография М. В. Болдина, Г. И. Симоновой и Ю. Н. Тюрина — заметный и весьма существенный вклад в статистическую литературу. Она безусловно окажет стимулирующее влияние на теоретиков и будет полезна всем тем, кто применяет непараметрические методы в прикладных статистических задачах.

СПИСОК ЛИТЕРАТУРЫ

1. *Puri M. L., Sen P. K.* Nonparametric Methods in General Linear Models. New York: Wiley, 1985, 399 p.
2. *Hettmansperger T. P.* Statistical Inference Based on Ranks. New York: Wiley, 1984, 323 p.
3. *Arbuthnott J.* An argument for divine providence taken from the constant regularity observed in the birth of two sexes. — *Philos. Trans.*, 1710, v. 27, p. 186–190.
4. *Boldin M. V., Simonova G. I., Tyurin Yu. N.* Sign-Based Methods in Linear Statistical Models. Providence, RI: Amer. Math. Soc., 1997.
5. *Nelson L. S.* A sign test for correlation. — *J. Qual. Technol.*, 1983, v. 15, № 4, p. 199–200.

24.XII.1998

Никитин Я. Ю.

Goldreich O ed. **Modern Cryptography, Probabilistic Proofs and Pseudorandomness**. Berlin–Heidelberg–New York: Springer-Verlag, 1999, xv + 182 p.

Три темы, составившие название книги и соответствующие названиям трех ее глав, несмотря на кажущуюся разнородность, тесно связаны друг с другом и с принципиальными основами теории вероятностей.

Слово «криптография» долгое время обозначало методы защиты государственных и военных тайн и неспециалистами произносилось с опаской. Однако с начала 80-х годов за рубежом стали открыто проводиться конференции по криптографии, и это слово стало привычным в западной научной литературе, а после изменения общественного строя — и в нашей стране. Причинами таких изменений стали по меньшей мере два обстоятельства: быстрое развитие электронных средств связи (удобных, но, как правило, полностью открытых для постороннего вмешательства) и необходимость надежной защиты переписки и конфиденциальной информации большого количества фирм, не доверяющих государственным органам, поскольку они могут находиться под влиянием конкурентов и транснациональных корпораций. Чтобы удовлетворить запросы расширившегося круга потребителей методов защиты информации, были использованы качественно новые идеи, предложенные криптографами, математиками и специалистами по вычислительным наукам. В результате «современная криптография» стала математически строгой наукой, тесно связанной с теорией вероятностных доказательств, и стимулировала разработку новых подходов к разработке понятия псевдослучайности.

Рецензируемая книга содержит строго (и в то же время доступно) написанные обзоры современного понимания трех этих тем, дает представление о важнейших понятиях, идеях, методах и результатах соответствующих теорий, представляющих интерес и для классических ветвей математики.

В первой главе книги «Основы современной криптографии» обсуждаются важнейшие особенности, отличающие современный подход к криптографии от классического. Криптография должна обеспечивать такое преобразование исходных сообщений, чтобы злоумышленник, перехвативший зашифрованное сообщение, не мог получить никакой информации об исходном (открытом) сообщении. Понимание теоретической секретности в классической и современной криптографии различается формализацией нестрогого выражения «не мог».

В классической криптографии схема совершенного шифрования была предложена Шенноном и предполагает, что открытое сообщение и способ шифрования выбираются независимо из множеств допустимых значений и обладают следующим свойством: условное распределение на множестве открытых текстов при фиксированном шифрованном тексте совпадает с безусловным распределением на множестве открытых текстов. Для практической реализации такой схемы необходимо (способом, гарантированно защищенным от злоумышленника) снабдить отправителя и получателя шифрованного сообщения вспомогательной информацией, объем которой не меньше объема зашифрованного сообщения (передаваемого по незащищенному каналу).

В «современной» криптографии подводится теоретическая база под естественное практическое понимание смысла выражения «не мог»: злоумышленнику, перехватившему шифрованное сообщение, чтобы получить хоть какую-нибудь информацию об открытом тексте, необходимо провести столь сложные вычисления, которые практически невозможно выполнить за разумное время. Формализация и теоретическое обоснование корректности такого определения потребовало существенного развития методов получения нижних оценок сложности алгоритмов и привело к построению аксиоматического понятия однонаправленной функции как последовательности функций $f_n(x)$, для которых сложность вычисления значения $y = f_n(x)$ растет при $n \rightarrow \infty$ по порядку существенно медленнее, чем время вычисления x по $y = f_n(x)$ (строгое определение этого понятия довольно громоздко). В практическом плане однонаправленные функции позволяют обеспечивать надежную защиту передаваемой информации даже без передачи вспомогательной информации по защищенному от злоумышленников каналу связи.

В первой главе приводятся сложившиеся к настоящему времени четкие определения основных понятий и процедур, используемых в современной криптографии: вычислительной сложности, вычислительной неразличимости, псевдослучайности, нулевого знания, шифрования, подписи, криптографических протоколов и т.п. — и обсуждаются относящиеся к ним теоремы и их неформальный смысл.

Содержание второй главы «Системы вероятностных доказательств» связано с современным подходом к привычному для математиков объекту: доказательству. Выясняется, что не только изобретение доказательства является нетривиальным актом, но и процедура проверки правильности доказательства не всегда тривиальна, и что эта процедура может стать совсем непростой, если на ее свойства наложить дополнительные ограничения.

Потребности защиты информации (возникшие в связи с ограничением доступа к электронным базам данных, использованием электронных кредитных карточек и т.п.) стимулировали разработку специфических процедур «доказательства» того, что клиент знает секретный пароль: кроме того, что «доказательства» должны обеспечить практически безошибочную многократную идентификацию клиента, они должны не позволять злоумышленнику, перехватывающему тексты «доказательств», в дальнейшем выдавать себя за клиента и пользоваться его правами. Основой таких процедур являются рассмотренные во второй главе интерактивные доказательства, доказатель-

ства с нулевым знанием, вероятно проверяемые доказательства и другие вероятностные системы доказательств. Важными элементами подобных «доказательств» являются случайный многоэтапный характер (это лишает злоумышленника возможности использовать уже реализованные варианты доказательств в будущем), наличие верхних ограничений на вычислительную сложность проверки каждого этапа доказательства (необходимого условия практической реализуемости) и нижних ограничений на сложность восстановления пароля по процедуре доказательства. Для построения процедур, удовлетворяющих последним двум условиям, используются однонаправленные функции.

Третья глава посвящена современной теории датчиков псевдослучайных чисел. Термин «псевдослучайная последовательность» предполагает существование понятия «случайная последовательность» и наличие какого-то различия между этими понятиями. Известно несколько подходов к определению случайной последовательности (в простейшем случае — случайной последовательности, элементы которой независимы и принимают значения 0 и 1 с вероятностью $\frac{1}{2}$). В обычной аксиоматической теории вероятностей такая последовательность понимается как последовательность измеримых функций на одном и том же пространстве элементарных событий (с заданными на нем σ -алгеброй измеримых множеств и вероятностной мерой), принимающих значения 0 и 1 и обладающих свойством взаимной независимости. При таком определении все двоичные последовательности оказываются совершенно равноправными (например, нулевая последовательность ничем не хуже последовательности знаков в записи числа π в двоичной системе счисления, хотя интуитивно ясно, что это не так). Различные определения случайности предлагались Мизесом и Черчем (на основе частотного подхода), Шенноном (как последовательности с максимальной энтропией), Колмогоровым, Соломоновым и Чайтиным (как последовательности с максимальным асимптотическим ростом длин программ, порождающих начальные отрезки последовательности).

В третьей главе книги излагается современный подход к определению псевдослучайности, основанный на идеализации конструкции датчиков псевдослучайных чисел, используемых в ЭВМ. Именно, датчиком псевдослучайных чисел называется последовательность детерминированных алгоритмов G_n , обладающих следующими свойствами:

а) алгоритм G_n применяется к двоичной строке U_n длины n и за полиномиально зависящее от n число операций порождает двоичную строку $G_n(U_n)$ длины $L(n)$,

б) если U_n — двоичная строка, образованная n независимыми случайными величинами, принимающими значения 0 и 1 с вероятностью $\frac{1}{2}$, то для любого полинома p , принимающего положительные значения, и для любой последовательности алгоритмов D_n , которые по двоичной строке длины $L(n)$ за полиномиально зависящее от n число операций вычисляют соответствующее ей значение, равное 0 или 1, существует такое k_0 , что при всех $k > k_0$

$$\left| \mathbf{P}\{D_k(G_k(U_k)) = 1\} - \mathbf{P}\{D_k(U_{L_k}) = 1\} \right| < \frac{1}{p(k)}.$$

Результаты исследований, проводившихся разными авторами, показали, что понятия однонаправленной функции и датчика псевдослучайных чисел эквивалентны: по каждому из этих объектов можно построить другой. В третьей главе обсуждаются различные модификации приведенного выше определения псевдослучайности и способы построения датчиков псевдослучайных чисел.

Таким образом, проблемы, рассматриваемые в трех главах книги, сводятся к использованию (в той или иной форме) однонаправленных функций. Это понятие является аксиоматическим (как понятие точки или прямой в геометрии) и, скорее всего, таким и останется. В настоящее время претендентами на воплощение основных свойств однонаправленных функций считаются специально конструируемые функции,

связанные с теоретико-числовыми задачами, сложность которых проверена многолетними исследованиями: разложение больших чисел на множители, решение уравнения $a^x = b$ или $x^2 = c$ в группах с достаточно сложной структурой. Следует отметить, что запросы упоминавшихся выше приложений стимулировали в последние десятилетия интенсивные теоретико-числовые исследования и заметно расширили проблематику теории чисел.

Кроме основных трех глав книга содержит 3 довольно больших приложения (Основы случайности и теории вычислений, Основные положения и результаты теории рандомизированных вычислений, Доказательство основной теоремы о предикате, эквивалентном по сложности однонаправленной функции), список библиографии на 357 названий и предметный указатель.

Книга написана достаточно строго (но с минимальным количеством определений и формул) и содержит много неформальных и исторических обсуждений рассматриваемых понятий. Книга допускает как «поверхностное» чтение, дающее общее представление о тематике, но и дает возможность понять многие особенности весьма нетривиальной теории. Этим она заметно отличается от весьма «технической» монографии [1], посвященной аналогичным вопросам.

В целом книга представляет значительный интерес для широкого круга читателей.

СПИСОК ЛИТЕРАТУРЫ

1. *Luby M.* Pseudorandomness and Cryptographic Applications. — Princeton Univ. Press, 1996.

27.V.1999

А. М. Зубков