ДОКЛАДЫ
АКАДЕМИИ НАУК СССР

1988

ТОМ 302 № 3

ОТДЕЛЬНЫЙ ОТТИСК

Приведем теперь достаточное условие выполнения неравенства (6).

Т е о р е м а 4. *Пусть A определено на открытом множестве U, $U \subset C[0, 1]$ и непрерывно дифференцируемо. Предположим, что в точке z (где $Az = 0$)*

$$f'(z) \in \operatorname{Isom}(C[0, 1], C[0, 1]).$$

Тогда существует окрестность U^* точки z, в которой выполняется неравенство

$$S \| Ax - Ay \| \geqslant \| x - y \|, \quad x, y \in U^*.$$

Д о к а з а т е л ь с т в о. По теореме о локальном обращении [3] существуют окрестности V точки 0 ($Az = 0$) и U' точки z такие, что A является C'-диффеоморфизмом U' на V и поэтому будут непрерывными отображения A^{-1} и $(A^{-1})'$. Тогда по теореме о конечных приращениях для A^{-1} будем иметь

$$(6) \qquad \| A^{-1}(\xi) - A^{-1}(\eta) \| \leqslant \sup_{0 \leqslant \tau \leqslant 1} \| (A^{-1})'((1 + \tau)\xi + \tau\eta) \| \cdot \| \xi - \eta \|$$

при всех ξ и η из окрестности V. Далее, в силу непрерывности $(A^{-1})'$ существует окрестность V', где $(A^{-1})'$ ограничено, т.е. $\exists S$ такое, что

$$\sup_{\theta \in V'} \| (A^{-1})'(\theta) \| \leqslant S;$$

тогда с учетом неравенства (6) получим

$$(7) \qquad \| A^{-1}(\xi) - A^{-1}(\eta) \| \leqslant S \| \xi - \eta \|, \quad \xi, \eta \in V'.$$

В силу непрерывности A можно выбрать U^* такую, что $\xi = Ax \in V'$, когда $x \in U^*$. Подставляя в (7) $\xi = Ax$ и $\eta = Ay$, получим

$$S \| Ax - Ay \| \geqslant \| x - y \|, \quad x, y \in U^*.$$

Институт вычислительной математики
Академии наук ГССР
Институт управления народным хозяйством
Тбилиси

Поступило
30 III 1987

ЛИТЕРАТУРА

1. *Колмогоров А.Н., Фомин С.В.* Элементы теории функций и функционального анализа. М.: Наука, 1981. 2. *Чичинадзе В.К.* Решение невыпуклых нелинейных задач оптимизации. М.: Наука, 1983. 3. *Картан А.* Дифференциальное исчисление. Дифференциальные формы. М.: Мир, 1971.

УДК 517.11

МАТЕМАТИКА

А.Х. ШЕНЬ

О СООТНОШЕНИЯХ МЕЖДУ РАЗЛИЧНЫМИ АЛГОРИТМИЧЕСКИМИ ОПРЕДЕЛЕНИЯМИ СЛУЧАЙНОСТИ

(Представлено академиком Ю.В. Прохоровым 14. VI 1988)

Существуют различные варианты определения понятия (индивидуального) случайного объекта средствами алгоритмической теории вероятностей. В настоящей статье исследуются соотношения между некоторыми из них. Именно в ней показано, что стохастические по Колмогорову–Лавлэнду последовательности могут не быть случайными в смысле определения Мартин–Лёфа [1, 2], а также что приведенная в [3] модификация определения Мартин–Лёфа ("случайность по Соловею") дает тот же класс случайных последовательностей, что и исходное определение Мартин–Лёфа. Доказательство первого факта проводится методом, предложенным М. Ламбальгеном [4].

1. В работе А.Н. Колмогорова [5] высказано утверждение, что существуют стохастические по Колмогорову–Лавлэнду (или, как еще говорят, случайные по Мизесу–Колмогорову–Лавлэнду) последовательности нулей и единиц (здесь и далее мы будем говорить о случайности относительно равномерной бернуллиевой меры, если не оговорено противное), энтропия начальных отрезков которых растет логарифмически. Такие последовательности не могут быть случайными по Мартин–Лёфу, так что из этого утверждения вытекает существование последовательностей, стохастических по Колмогорову–Лавлэнду, но не случайных по Мартин–Лёфу. Однако доказательство этого утверждения Колмогорова не было опубликовано, и, как недавно показал Ан.А. Мучник, это утверждение неверно: всякая последовательность, энтропия начальных отрезков которой длины n не превосходит $Cn + O(1)$ для некоторого $C < 1$, не является стохастической по Колмогорову–Лавлэнду. (Мы не оговариваем точно, какой именно вариант энтропии рассматривается, так как разница между ними не превосходит по порядку логарифма длины последовательности и в данном случае несущественна; подробнее см. в [2, 6].)

Однако существование стохастических, но не случайных последовательностей может быть доказано иным путем. Ниже приводится доказательство, использующее методы работы [4].

Теорема 1. *Существует стохастическая по Колмогорову–Лавлэнду относительно равномерной бернуллиевой меры последовательность, не являющаяся случайной по Мартин–Лёфу относительно той же меры.*

Доказательство. Следуя М. Ламбальгену, рассмотрим последовательность вещественных чисел $p = p_0, p_1, \ldots$, сходящуюся к ½, но достаточно медленно. Рассмотрим меру μ_p на пространстве всех двоичных последовательностей, соответствующую независимым испытаниям, в i-м из которых вероятность появления 1 равна p_i. Рассмотрим случайную по Мартин–Лёфу относительно этой меры последовательность. Оказывается, что она будет стохастической относительно равномерной меры, но не будет случайной относительно нее. Перейдем к более подробному изложению.

Лемма 1. *Пусть $p = p_0, p_1, \ldots$ – вычислимая последовательность вычислимых действительных чисел, причем ряд $\Sigma(p_i - ½)^2$ расходится. Тогда классы случайных по Мартин–Лефу последовательностей по равномерной мере и по мере μ_p не пересекаются.*

Доказательство. Утверждение леммы следует из более общих результатов В.Г. Вовка [7]; мы приведем его доказательство для интересующего нас случая. Наряду с мерой μ_p и равномерной мерой (обозначим ее $\mu_{1/2}$) рассмотрим третью меру μ', в которой вероятности появления единиц будут средними арифметическими чисел p_i и ½. Пусть последовательность ω случайна по мерам μ_p и $\mu_{1/2}$ одновременно. Через u_i обозначим вероятность появления i-го члена последовательности ω по мере μ_p (т.е. $u_i = p_i$, если i-й член последовательности ω равен 1, и $u_i = 1 - p_i$ в противном случае). Через v_i и w_i обозначим аналогичные вероятности для мер $\mu_{1/2}$ и μ' (так что $v_i = ½$, а $w_i = (u_i + v_i)/2$). Критерий случайности в терминах априорной вероятности (см. [8]) позволяет утверждать, что

$$\prod_{i=1}^{n} w_i \leqslant C \prod_{i=1}^{n} u_i, \qquad \prod_{i=1}^{n} w_i \leqslant C \prod_{i=1}^{n} v_i$$

для некоторого C и для любого n. (Мы пользуемся тем, что мера μ' не превосходит априорной вероятности.) Перемножая эти неравенства и переходя к логарифмам, мы видим, что

$$\Sigma \log ((u_i + v_i)/2) \leqslant \Sigma (\log u_i + \log v_i)/2 + O(1).$$

Разница между слагаемыми в левой и правой частях имеет порядок $(u_i - v_i)^2$ (выпуклость логарифма); отсюда следует, что ряд, фигурирующий в утверждении леммы, сходится.

Лемма 2. *Пусть $p_0, p_1, \ldots$ — вычислимая последовательность вычислимых действительных чисел, вычислимо сходящаяся к ½. Тогда любая случайность по Мартин–Лёфу последовательность по мере μ_p является стохастической по Колмогорову–Лавлэнду относительно равномерной меры.*

Доказательство. Пусть это не так и ω — случайная по Мартин–Лёфу последовательность, не являющаяся стохастической, R — соответствующее правило выбора. Выберем такое $\epsilon > 0$, чтобы частота единиц в выбранной с помощью правила R подпоследовательности бесконечно много раз превосходила ½ + ϵ. (Случай, когда она бесконечно много раз меньше ½ − ϵ, аналогичен.) Мы придем к противоречию, если покажем, что множество тех последовательностей, для которых частота единиц в выбранной с помощью правила R подпоследовательности бесконечно много раз бывает больше ½ + ϵ, является эффективно нулевым (относительно меры μ_p).

Обозначим A_N множество тех последовательностей, для которых применение правила R дает подпоследовательность не менее чем из N членов и частота единиц среди первых N ее членов превосходит ½ + ϵ. Достаточно показать, что ряд $\mu_p(A_N)$ вычислимо сходится (т.е. по заданному $\delta > 0$ можно эффективно указать его частную сумму, отстоящую от суммы ряда не более чем на δ). (Из приводимой далее теоремы 2 будет следовать, что достаточно установить его сходимость.)

Обозначим теперь $\alpha_{N,k}(q_1, \ldots, q_N)$ вероятность того, что при N независимых испытаниях, вероятности появления единицы в которых равны $q_1, \ldots, q_N$, число единиц превосходит k. Очевидно, что функция $\alpha_{N,k}$ неубывает по всем аргументам и $\alpha_{N,k} \leqslant \alpha_{N,l}$ при $k \geqslant l$. Мы утверждаем, что $\mu_p(A_N)$ не превосходит $\alpha_{N,k}(q_1, \ldots, q_N)$, где $k = N(1/2 + \epsilon)$, а q_i — i-й по величине член последовательности $p_0, p_1, \ldots$ (q_1 — максимальный, q_2 — максимальный из оставшихся и т.д.; если таковых нет, то q_1 — точная верхняя грань членов последовательности, q_2 — точная верхняя грань минимумов пар членов последовательности и т.д.).

Покажем, как из этой оценки получить требуемое утверждение про сходимость ряда $\Sigma\mu_p(A_N)$. Очевидно, $\lim q_i$ = ½. Заменим те q_i, которые больше ½ + $\epsilon/2$ (пусть их количество равно 1), на 1, а остальные на ½ + $\epsilon/2$. Получим

$$\mu_p(A_N) \leqslant \alpha_{N-s,\, k-s}(½ + \epsilon/2, \ldots, ½ + \epsilon/2).$$

После этого остается, воспользовавшись стандартной оценкой (теоремой Муавра–Лапласа, формулой Стирлинга и т.п.), убедиться, что $\mu_p(A_N)$ экспоненциально убывает с ростом N.

Докажем теперь, что $\mu_p(A_N) \leqslant \alpha_{N,k}(q_1, \ldots, q_N)$. Будем представлять себе, как это описано в [9], что члены последовательности написаны на карточках, лежащих лицом вниз, и что правило выбора говорит, какие карточки нужно перевернуть для просмотра и какие — для включения в выбранную подпоследовательность. При этом сведения о том, какие карточки и с какой целью переворачивались, записываются и составляется протокол применения правила выбора к данной подпоследовательности. Пусть π — начальный отрезок такого протокола. $N(\pi)$ обозначим количество членов, включенных в подпоследовательность на отрезке π, $k(\pi)$ — количество единиц среди этих членов. Через $q_i(\pi)$ обозначим i-й по величине член последовательности, получаемой из $p_0, p_1, \ldots$ выкидыванием членов, соответствующих выбранным (для просмотра или включения в подпоследовательность) карточкам на отрезке π. Через $\mu_p(A_N|\pi)$ обозначим условную вероятность (относительно меры μ_p) события A_N при условии, что протокол применения правила выбора R начинается на π. Мы докажем следующее обобщение интересующего нас неравенства: при $N(\pi) \leqslant N$

$$(1) \qquad \mu_p(A_N|\pi) \leqslant \alpha_{N-N(\pi),k-k(\pi)}(q_1(\pi),\ldots)$$

(при пустом π получаем исходное). Если $N(\pi) = N$, неравенство (1) превращается в равенство (левая и правая его части одновременно равны либо 0, либо 1). Пусть $N(\pi) < N$, s – номер карточки, переворачиваемой следующей после π (если такой нет, то $\mu_p(A_N|\pi) = 0$). Тогда

$$(2) \qquad \mu_p(A_N|\pi) = p_s\mu_p(A_N|\pi_1) + (1-p_s)\mu_p(A_N|\pi_0),$$

где π_1 и π_0 – протоколы, получающиеся добавлением к π информации о единице (соответственно, нуле) на s-й карточке. Покажем, что если неравенство (1) верно для π_1 и π_0, то оно верно и для π. Правая часть (2) не превосходит

$$(3) \qquad p_s\alpha_{N-N(\pi_1),k-k(\pi_1)}(q_1(\pi_1),\ldots) + (1-p_s)\alpha_{N-N(\pi_0),k-k(\pi_0)}(q_1(\pi_0),\ldots).$$

Если s-я карточка была выбрана только для просмотра, то $N(\pi_1) = N(\pi_0) = N(\pi)$, $k(\pi_1) = k(\pi_0) = k(\pi)$ и остается воспользоваться монотонностью $\alpha_{N,k}$ и тем, что $q_i(\pi_0) = q_i(\pi_1) \leqslant q_i(\pi)$. Если же s-я карточка включена в подпоследовательность, то $N(\pi_1) = N(\pi_0) = N(\pi) + 1$, $k(\pi_1) = k(\pi_0) + 1$, $k(\pi_0) = k(\pi)$ и выражение (3) равно

$$\alpha_{N-N(\pi),k-k(\pi)}(p_s, q_1(\pi_0), q_2(\pi_0),\ldots)$$

и тем самым не превосходит $\alpha_{N-N(\pi),k-k(\pi)}(q_1(\pi),\ldots)$.

Это завершает доказательство неравенства (1) в случае, когда все начальные отрезки протоколов π с $N(\pi) = N$ имеют ограниченную длину. Если же это не так, приведенные рассуждения позволяют получить оценку для $\mu_p(A_{Nt})$, где A_{Nt} – множество тех последовательностей, где после не более чем t переворачиваний карточек получается подпоследовательность длиной не менее N и частотой единиц в начальном отрезке длины N больше $\frac{1}{2} + \epsilon$. Остается лишь перейти к пределу при $t \to \infty$. Доказательство леммы 2 завершено.

Теперь для доказательства теоремы осталось лишь выбрать вычислимую последовательность вычислимых действительных чисел $p_0, p_1, \ldots$, вычислимо сходящуюся к $\frac{1}{2}$, для которой ряд $\Sigma(p_i - \frac{1}{2})^2$ расходится. Это можно сделать, например, положив $p_i = \frac{1}{2} + 1/\sqrt{i+10}$.

2. В работе [3] приведено следующее определение случайности последовательности по вычислимой мере на пространстве всех бесконечных последовательностей нулей и единиц. (Строго говоря, в [3] идет речь о случайности действительных чисел, но все сказанное легко переносится и на последовательности нулей и единиц.)

Определение. Последовательность ω случайна по Соловею, если для всякой вычислимой последовательности эффективно открытых множеств, сумма мер которых конечна, лишь конечное число из них содержат последовательность ω. (Эффективно открытое множество – объединение перечислимого множества интервалов; интервал – множество всех бесконечных продолжений некоторой конечной последовательности.)

Как указано в [3], всякая случайная по Соловею последовательность случайна по Мартин-Лёфу. Там же отмечено, что если в определении случайности по Соловею потребовать, чтобы ряд, составленный из мер эффективно открытых множеств, не просто сходился, а вычислимо сходился, то определение станет эквивалентным определению Мартин-Лёфа.

Следующая теорема показывает, что и без этой модификации случайность по Соловею равносильна случайности по Мартин–Лёфу, тем самым отвечая на поставленный в [3] вопрос.

Теорема 2. *Всякая случайная по Мартин–Лёфу относительно некоторой вычислимой меры последовательность случайна по Соловею относительно той же меры.*

Доказательство. Предположим, что некоторая последовательность ω не случайна по Соловею относительно некоторой вычислимой меры μ на пространстве всех бесконечных последовательностей нулей и единиц. Тем самым существуют эффективно открытые множества $U_0, U_1, \ldots$, для которых $S = \Sigma\mu(U_i) < < \infty$, а $\omega \in U_i$ при бесконечно многих i. Мы покажем, что последовательность ω не случайна по Мартин–Лёфу, указав способ для каждого $\epsilon > 0$ построить эффективно открытое множество, содержащее ω и имеющее меру не более ϵ.

Пусть n – произвольное положительное целое число. Рассмотрим множество V_n, состоящее из тех бесконечных последовательностей, которые принадлежат по крайней мере n из множеств U_i. Множество V_n является эффективно открытым: если некоторая последовательность ему принадлежит, то это рано или поздно удастся обнаружить по ее начальным отрезкам, найдя n различных чисел i, при которых $\omega \in U_i$. Легко видеть также, что мера множества V_n не превосходит S/n. (Сумма характеристических функций множеств U_i по всем i имеет интеграл S, а на множестве V_n ограничена снизу числом n.) Последовательность ω, по нашему предположению, принадлежит множеству V_n при любом n. Таким образом, чтобы получить эффективно открытое множество меры не более ϵ, содержащее последовательность ω, достаточно выбрать n таким, чтобы $S/n < \epsilon$, и взять множество V_n. Заметим, что возможная невычислимость действительного числа S не является при этом помехой, так как мы можем пользоваться любой оценкой сверху для S. Теорема 2 доказана.

Автор благодарит Е.А. Асарина, Н.К. Верещагина, В.Г. Вовка, В.В. Вьюгина, Ан.А. Мучника, Б.И. Пенкова, А.Л. Семенова, В.А. Успенского и всех участников семинара А.Н. Колмогорова.

Институт проблем передачи информации
Академии наук СССР,
Москва

Поступило
21 VI 1988

ЛИТЕРАТУРА

1. *Kolmogorov A., Uspensky V.* Proc. of the I world congress of the Bernoulli society. Utrecht. The Netherlands. 1987, vol. 1, p. 3–53. 2. *Успенский В.А., Семенов А.Л.* Теория алгоритмов: основные открытия и приложения. М.: Наука, 1987. 3. *Chaitin G.* Adv. Appl. Math., 1987, vol. 8, p. 119–146. 4. *van Lambalgen M.* Random sequences. Amsterdam: Acad. Proefschrift. 1987. 5. *Колмогоров А.Н.* Проблемы передачи информации. 1969, т. 5, вып. 3, с. 3–7. 6. *Шень А.Х.* ДАН, 1984, т. 276, № 3, с. 563–566. 7. *Вовк В.Г.* – ДАН, 1987, т. 294, № 6, с. 1298–1302. 8. *Вьюгин В.В.* Семиотика и информатика. М.: ВИНИТИ, 1981, вып. 16, с. 14–43. 9. *Шень А.Х.* Там же, 1982, вып. 18, с. 14–42.