

# Равномерные тесты случайности

По рассказам В. Вьюгина по статье Гача

## 1 Перечислимые снизу функции на $\Omega$

Пусть  $t$  — функция, определённая на множестве  $\Omega$  бесконечных последовательностей нулей и единиц и принимающая неотрицательные действительные значения и значение  $+\infty$ . Она называется *перечислимой снизу*, если для любого рационального числа  $r$  множество

$$\{\omega \mid r < f(\omega)\}$$

открыто, то есть представляет собой объединение множеств вида  $\Omega_x$  (здесь  $\Omega_x$  — множество всех последовательностей, начинающихся на конечное слово  $x$ ), и, более того, *эффективно открыто равномерно по  $r$* . Последнее означает, что существует алгоритм, который получает на вход рациональное  $r$  и выдаёт на выход по очереди слова  $x_0, x_1, \dots$ , для которых объединение интервалов  $\Omega_{x_i}$  совпадает с  $\{\omega \mid r < t(\omega)\}$ .

Это определение является конструктивным вариантом классического определения полунепрерывной снизу функции (где требуется лишь открытость, но не эффективная открытость).

Тот же класс функций можно определить и другими способами.

Функцию  $u$ , определённую на  $\Omega$  и принимающую рациональные значения, назовём *простой*, если её значение  $u(\omega)$  определяется конечным числом членов последовательности  $\omega$  (некоторым начальным отрезком). Такие функции можно задавать таблицей значений для разных вариантов начального отрезка и считать конструктивными объектами.

Далее можно рассматривать неубывающие (поточечно) вычислимые последовательности простых функций. Их (поточечные) пределы и являются перечислимыми снизу функциями на  $\Omega$ .

Переходя к разностям (разность двух простых функций будет простой), можно сказать так: полу-непрерывные снизу функции — это суммы вычислимых рядов, составленных из неотрицательных простых функций.

Ещё один способ задать перечислимую снизу функцию на  $\Omega$  таков. Рассмотрим произвольную перечислимую снизу функцию  $T$  на множестве  $\Sigma$  конечных последовательностей нулей и единиц, принимающую неотрицательные (конечные или бесконечные) значения. (Перечислимость снизу понимается в обычном смысле: множество пар  $(x, r)$ , для которых  $r < T(x)$ , перечислимо.) Теперь определим функцию  $t$  на  $\Omega$  так:

$$t(\omega) = \sup\{T(x) \mid x — начало \omega\}$$

Эта функция будет перечислимая снизу.

Всякая перечислимая снизу функция на  $\Omega$  может быть получена таким способом. Более того, можно наложить дополнительные условия на функцию  $T$ . Например, можно считать её монотонной (если  $x$  — начало  $y$ , то  $T(x) \leq T(y)$ ), достаточно перейти от  $T(x)$  к максимуму  $T(z)$  по всем  $z$ , являющимся началом  $x$ .

Можно считать  $T$  вычислимой функцией с рациональными значениями. (В самом деле, поскольку нас интересует лишь точная верхняя грань  $T$  на всех началах, вместо увеличения значения  $T(x)$  для некоторого  $x$  можно увеличить это значение на всех продолжениях слова  $x$  достаточно большой длины  $N$ ; это отложенное увеличение позволяет считать  $T$  вычислимой.)

По соображениям компактности среди всех перечислимых снизу функций  $T$  на конечных словах, задающих данную перечислимую снизу функцию  $t$  на бесконечных последовательностях, существует максимальная. А именно, можно рассмотреть функцию

$$T(x) = \inf\{t(\omega) \mid \omega \text{ начинается на } x\}$$

Она будет перечислимой снизу. В самом деле,  $r < T(x)$  тогда и только тогда, когда существует  $r' > r$ , для которого  $r' < t(\omega)$  для всех  $\omega$ , начинающихся на  $x$ . Последнее можно переформулировать так: открытое множество тех последовательностей  $\omega$ , для которых  $t(\omega) > r'$ , содержит  $\Omega_x$ . Это открытое множество задано нам как объединение пере-

числимого семейства интервалов; если они покрывают  $\Omega_x$ , то это обнаружится на конечном шаге, значит, указанное свойство перечислимо (и квантор существования по  $r'$  не нарушает перечислимости).

**Замечание.** Последнее рассуждение существенно использует компактность и не проходит, если вместо последовательностей нулей и единиц рассматривать, скажем, последовательности натуральных чисел. (Но определение перечислимой снизу функции и предыдущие рассуждения на этот случай переносятся.)

## 2 Тесты случайности

Пусть на пространстве  $\Omega$  задана вычислимая вероятностная мера мера  $P$ . Перечислимую снизу функцию  $t$  на  $\Omega$  (с неотрицательными значениями, возможно, бесконечными) будем называть *тестом случайности* относительно меры  $P$ , если математическое ожидание функции  $t$  по мере  $P$  не превосходит единицы, то есть

$$\int t(\omega) dP(\omega) \leq 1.$$

(Интуитивный смысл: чем больше  $t(\omega)$ , тем больше тест  $t$  находит “закономерностей” в последовательности  $\omega$ . Строя тест, мы можем объявлять закономерностями что угодно, но должны “соблюдать меру”: если закономерностей будет слишком много, то математическое ожидание станет бесконечным.)

Последовательность  $\omega$  проходит тест  $t$ , если  $t(\omega) < \infty$ . Последовательность будем считать случайной, если она проходит все тесты. Как мы увидим, это определение совпадает со случайностью по Мартин-Лёфу, поскольку тест в некотором смысле заменяет семейство покрытий уменьшающихся мер. Но сначала докажем теорему, аналогичную теореме о существовании максимального эффективно нулевого множества.

**Теорема.** Для любой вычислимой меры  $P$  существует максимальный тест  $u$  относительно  $P$ : для любого другого теста  $t$  относительно  $P$  найдётся константа  $c$ , для которой

$$t(\omega) \leq cu(\omega)$$

для любой последовательности  $\omega \in \Omega$ .

(В частности  $u(\omega)$  конечно, если и только если все  $t(\omega)$  конечны, так что этот тест проходят случайные последовательности и только они.)

**Доказательство.** Будем перечислять алгоритмы, задающие полунепрерывные снизу функции. Каждый такой алгоритм порождает монотонную последовательность простых функций. Прежде чем выпустить очередную простую функцию в свет, будем убеждаться, что её математическое ожидание по мере  $P$  меньше 2. (Если алгоритм задаёт тест, то математическое ожидание не больше 1, и потому, вычислив значения меры  $P$  с достаточной точностью, мы сможем убедиться, что оно меньше 2.) Если убедиться не удалось, то на этом последовательность простых функций обрывается.

Таким образом, мы перечислим все тесты, а также некоторые не совсем тесты, но не более чем вдвое превосходящие тесты. Остается сложить все функции с положительными коэффициентами, сумма которых не превосходит  $1/2$  (скажем  $1/2^{i+2}$ ).

**Теорема.** Последовательность проходит все тесты (проходит универсальный тест) тогда и только тогда, когда она случайна по Мартин-Лёфу.

**Доказательство.** Если  $t$  — тест, то множество тех последовательностей  $\omega$ , для которых  $t(\omega) > N$ , эффективно открыто, может быть эффективно указано по  $N$  и имеет меру не больше  $1/N$ , так что не проходящая тест последовательность (для которой  $t$  бесконечно) содержится в эффективно нулевом множестве.

С другой стороны, для всякого эффективно нулевого множества  $N$  можно построить тест, который бесконечен на всех элементах этого множества. В самом деле, для любого эффективно открытого множества  $U$  функция  $\chi_U$ , равная единице внутри  $U$  и нулю в остальных точках, перечислимая снизу. Обозначим через  $U_\varepsilon$  эффективно открытое множество, содержащее  $N$  и имеющее меру меньше  $\varepsilon$ . Теперь в качестве теста можно взять сумму

$$\sum_i c_i \chi_{U_{\varepsilon_i}},$$

где  $c_i$  стремятся к бесконечности, а  $\varepsilon_i$  к нулю, причём быстрее, так что  $\sum c_i \varepsilon_i < 1$ .

**Замечание.** Можно сменить шкалу на логарифмическую, определив  $d(\omega)$  равенством

$$u(\omega) = 2^{d(\omega)}$$

(где  $u$  — универсальный тест). Функция  $d$  перечислима снизу и максимальна (с точностью до аддитивной константы) среди перечислимых снизу

функций, у которых математическое ожидание величины  $2^{d(\omega)}$  конечно. Функция  $d$ , так сказать, измеряет дефект случайности в битах, и определена с точностью до аддитивной константы. Заметим, что можно считать  $d$  неотрицательной, так как можно рассматривать лишь функции  $t$ , не меньшие единицы (прибавление константы не влияет на конечность интеграла). Также можно без ограничения общности предполагать, что функция  $d$  имеет целые значения.

Как мы видели, дефект последовательности конечен тогда и только тогда, когда она случайна по Мартин-Лёфу.

**Замечание:** в отличие от характеризации с помощью монотонной или априорной сложности, критерий случайности с помощью тестов заведомо инвариантен относительно вычислимых перестановок последовательности.

### 3 Префиксный и обычный дефект

Приведённое определение дефекта напоминает определение префиксной сложности. Можно дать и другое определение, которое больше похоже на обычную сложность. А именно, будем требовать, чтобы мера множества всех последовательностей, для которых тест больше  $N$ , не превосходила  $1/N$ . (Очевидно, это свойство более слабое, то есть выполнено для всех функций с математическим ожиданием не больше 1 — неравенство Чебышёва).

В логарифмической шкале это выглядит так: мера множества тех последовательностей, где дефект больше  $n$ , не больше  $2^{-n}$ .

Строя универсальный тест, удобно пользоваться логарифмической шкалой и ограничиваться целыми значениями  $n$ . Надо, как и раньше, перечислять все тесты  $d_i$  (при этом могут попасть и не только тесты, но почти тесты) и затем взять взвешенный максимум:

$$d(\omega) = \max_i [d_i(\omega) - i] - c$$

При этом  $d$  уступает  $d_i$  не более чем на  $i$ , а множество тех  $\omega$ , где  $d(\omega) > k$ , есть объединение множеств, где  $d_i(\omega) > k + i + c$ , их меры не больше  $O(2^{-k-i-c})$ , и при подходящем  $c$  сумма мер будет меньше  $2^{-k}$ , что и требовалось.

Возникают две “меры неслучайности”, которые можно назвать префиксным дефектом  $d_P$  и обычным дефектом  $d_S$ . Обе они задают одно и то

же множество неслучайных последовательностей (как множество последовательностей бесконечного дефекта). Оказывается, что и конечные значения этих дефектов связаны друг с другом. В одну сторону это очевидно: всякий префиксный тест является обычным тестом, так что

$$d_P(\omega) \leq d_S(\omega) + O(1).$$

В обратную сторону неравенство менее точное:

**Теорема.**

$$d_S(\omega) \leq d_P(\omega) + 2 \log d_P(\omega) + O(1).$$

**Доказательство.** Пусть  $d$  — обычный тест (в логарифмической шкале). Покажем, что  $d - 2 \log d$  является префиксным тестом. Вероятность того, что  $d(\omega)$  находится между  $i$  и  $i + 1$ , не превосходит  $1/2^i$ , интеграл от  $2^{d-2 \log d}$  по этому множеству оценивается как  $2^{-i} 2^{i-2 \log i} = 1/i^2$  и потому общий интеграл конечен.

Осталось заметить, что неравенство  $a < b + 2 \log b + O(1)$  следует из  $b > a - 2 \log a - O(1)$  (если  $b > a$ , то всё и так ясно; если  $a < b$ , то  $\log a < \log b$ ).

**Замечание.** Принципиальная разница этого утверждения с утверждением о связи обычной и префиксной энтропии состоит в том, оценка погрешности выражается через дефект случайности (и потому мала для последовательностей, близких к случайным), а не через сложность (как обычно).

### 4 Формула для префиксного дефекта

Для универсального теста случайности  $u$  (в префиксном смысле, с математическим ожиданием) имеется следующая формула, выражающая его через априорную вероятность (и тем самым префиксную сложность):

**Теорема**

$$u(\omega) = \sum \{m(x)/P(x) \mid x — начало \omega\}$$

где  $m(x)$  — априорная вероятность (на изолированных словах, не на дереве — другими словами,  $m(x) = 2^{-KP(x)}$ ), а  $P(x)$  — мера множества  $\Omega_x$ .

(Равенство здесь понимается с максимально разумной точностью: до ограниченного и отделённого от нуля множителя.)

**Доказательство.** Поскольку  $m$  перечислима снизу, а  $P$  вычислима (и потому  $1/P$  перечислима снизу), то сумма в правой части является перечислимой снизу функцией на  $\Omega$ . Проверим, что

её математическое ожидание конечно. В самом деле, математическое ожидание есть сумма по  $n$  математических ожиданий функций, которые получатся, если в формуле оставить суммирование по словам длины  $n$ . Но каждое такое ожидание равно  $\sum m(x)$  по словам длины  $n$  (мера множества  $\Omega_x$  сокращается с  $P(x)$  в знаменателе), и в сумме получится  $\sum m(x)$  по всем  $x$ , а эта сумма конечна.

Обратное неравенство. Функция  $u$  представима в виде суммы вычислимого ряда из простых функций. Каждую простую функцию можно представить в виде суммы характеристических функций интервалов с рациональными коэффициентами, поэтому  $u$  есть сумма (вычислимого) ряда из характеристических функций интервалов с рациональными коэффициентами. Пусть  $x_k$  — корень  $k$ -го интервала, а  $r_k$  — коэффициент при соответствующей характеристической функции. Это означает, другими словами, что

$$u(\omega) = \sum \{r_k \mid x_k \text{ — начало } \omega\}.$$

Конечность математического ожидания  $u$  означает, что

$$\sum r_k P(x_k) < \infty,$$

откуда  $m(k) \geq r_k P(x_k)$ , где  $m(k)$  — априорная вероятность числа  $k$ . Предположим для начала, что все  $x_k$  различны (этого легко добиться, заменив их на продолжения; впрочем, как мы увидим, без этого предположения можно и обойтись). Поскольку функция  $k \mapsto x_k$  вычислена, то

$$m(x_k) \geq m(k) \geq r_k P(x_k),$$

или

$$r_k \leq \frac{m(x_k)}{P(x_k)}.$$

Сложив эти неравенства для всех  $x_k$ , являющихся началами некоторой последовательности  $\omega$ , находим, что

$$u(\omega) \leq \sum \{m(x)/P(x) \mid x \text{ — начало } \omega\}.$$

(все неравенства понимаются с точностью до константы).

Здесь использовано, что все  $x_k$  различны (так как в сумме в правой части выражение каждое начало  $x$  встречается один раз, а в сумме для  $u(\omega)$  могло быть несколько членов с одним и тем же  $x_k$ ). Если не все  $x_k$  различны, то получится лишь

$$u(\omega) \leq \sum \{m(k)/P(x_k) \mid x_k \text{ — начало } \omega\},$$

и далее можно воспользоваться тем, что сумма  $m(k)$  по всем  $k$ , для которых  $x_k$  равно некоторому слову  $x$ , не больше  $m(x)$  (поскольку образ меры  $m$  при вычислимом отображении не больше априорной вероятности).

В это теореме вместо суммы можно написать точную верхнюю грань:

### Теорема

$$u(\omega) = \sup \{m(x)/P(x) \mid x \text{ — начало } \omega\}$$

**Доказательство.** Ясно, что правая часть стала только меньше, так что в модификации нуждается лишь вторая часть доказательства.

Рассмотрим функции  $u_i$ , для которых  $u_i(\omega) = 2^i$ , если  $u(\omega) > 2^i$ , и нуль в противном случае. Сумма величин  $u_i(\omega)$  по всем  $i$  отличается от  $u(\omega)$  не более чем в два раза раз (в обе стороны), если  $u(\omega)$  не слишком мало (а малые значения не важны, так как не влияют на конечность интеграла).

Каждая функция  $u_i$  есть  $2^i$ , умноженное на характеристическую функцию эффективно открытого множества, которое есть счётное объединение непересекающихся интервалов. Таким образом,  $u_i$  есть  $2^i$ , умноженную на ряд из характеристических функций этих интервалов. В сумме получается ряд для  $u$  (точнее, для близкой к ней функции) из сумм характеристических функций интервалов с коэффициентами, в котором все ненулевые (в данной точке) члены суть различные степени двойки.

Далее всё рассуждение проходит как раньше, но только надо ещё заметить, что для ряда из различных степеней двойки (а мы позаботились, чтобы они были различны) максимум и сумма отличаются не более чем в два раза. Теорема доказана.

**Следствие.** Последовательность  $\omega$  случайна тогда и только тогда, когда для её начальных отрезков разность  $\log_2 P(x) - K P(x)$  ограничена сверху.

(В самом деле, только что доказанная теорема утверждает, что максимум этой разности по всем начальным отрезкам есть префиксный дефект случайности.)

Тем самым получается доказательство теоремы Левина — Шнорра в варианте с префиксной сложностью (причём, в отличие от обычного доказательства, префиксная сложность возникает здесь естественно, а не как побочный продукт рассуждения.)

## 5 Тесты и сложности

Доказанные теоремы выражают дефект случайности (значение универсального теста) через сложность, но лишь для бесконечных последовательностей. Возникает естественный вопрос: что можно сказать о конечных последовательностях и нельзя ли, скажем, связать сложность конечной последовательности и дефект случайности её продолжений?

Кое-что на эту тему сказать можно. Как получить функцию на конечных последовательностях, начав с универсального теста случайности  $u$  (в префиксном варианте)?

Можно определить функцию  $\bar{u}$  на конечных последовательностях, положив  $\bar{u}(z)$  равным минимальному дефекту всех продолжений, то есть

$$\inf\{u(\omega) \mid \omega \text{ — бесконечное продолжение } z\}$$

Как мы уже говорили, эта функция перечислена снизу (для последовательностей нулей и единиц, см. выше) и позволяет восстановить  $u$ , так что её можно рассматривать как вариант представления функции  $u$ , избегающих бесконечных последовательностей.

Другой способ получить функцию на конечных последовательностях — рассмотреть условное математическое ожидание функции  $u$  на продолжениях слова  $z$  (по мере  $P$ ).

Другими словами, мы рассматриваем функцию  $U$ , для которой  $U(z)$  равно интегралу функции  $u$  по мере  $P$ , ограниченной на продолжения слова  $z$ . Эта функция является перечислимой снизу полумерой (и даже мерой, вот только мера всего пространства не обязательно равна единице). Затем мы полагаем  $\hat{u}(z)$  равным отношению  $U(z)/P(z)$ .

### Теорема

$$\frac{m(z)}{P(z)} \leq \bar{u}(z) \leq \hat{u}(z) \leq \frac{A(z)}{P(z)},$$

где  $m$  — априорная вероятность на изолированных словах, а  $A$  — априорная вероятность на дереве.

(Все неравенства понимаются с точностью до мультиплективной константы.)

В самом деле, первая часть следует из формулы для  $u(\omega)$ : для всех  $\omega$ , продолжающих  $z$ , в сумму входит слагаемое  $m(z)/P(z)$ . Во втором неравенстве минимум не превосходит математического ожидания. Наконец, последнее неравенство вытекает из сравнения перечислимой снизу полумеры  $T(z)$  с максимальной полумерой  $A(z)$ .

В логарифмической шкале это неравенство записывает так:

$$\begin{aligned} -\log P(x) - KP(x) &\leq \log \bar{u}(z) \leq \\ &\leq \log \hat{u}(z) \leq -\log P(x) - KA(x) \end{aligned}$$

Заметим ещё, что мера  $T$  может зависеть от  $P$  (поскольку по существу рассматривается максимум в классе мер, имеющих плотность относительно  $P$ ). Но эта зависимость не может быть особенно сильной: приведённое неравенство показывает, что возможные колебания ограничены разностью между  $KP(x)$  и  $KA(x)$ .

**Замечание.** Правый знак неравенства нельзя заменить на равенство. Рассмотрим, скажем, равномерную меру в качестве  $P$ . Соответствующая ей величина  $T(z)$  стремится к нулю, когда  $z$  является удлиняющимся началом вычислимой последовательности (поскольку берётся интеграл по множествам, пересечение которых состоит из единственной точки, а точка имеет нулевую меру относительно  $P$ ). С другой стороны,  $A(z)$  остаётся отделённой от нуля для таких  $z$ .

Вопрос: можно ли сказать что-нибудь про остальные знаки неравенств? И зависит ли  $T$  от выбора  $P$ ?

## 6 Бернуlliевые последовательности

Можно определять случайность не только относительно одной меры, но и относительно семейства мер. Наиболее естественный пример такого рода — семейство бернуlliевых мер, соответствующих независимым бросаниям монеты, у которой вероятность выпадения единицы равна  $p$ , где  $p$  — некоторое действительное число в отрезке  $[0, 1]$ . (Заметим, что рассматриваются все значения  $p$ , не только вычислимые.) Неформально говоря, нам дают последовательность и говорят, что она получена в результате независимых бросаний монеты (возможно, несимметричной); мы должны сказать, мыслимо ли это.

Будем говорить, что множество  $A \subset \Omega$  является эффективно нулевым относительно семейства бернуlliевых мер, если существует алгоритм, который по каждому рациональному  $\varepsilon > 0$  указывает последовательность интервалов, которая покрывает  $A$  и сумма мер которых при любом  $p$  не превосходит  $\varepsilon$ .

Вопрос: если мы откажемся от требования эффективности, то равносильно ли это тому, что любая бернуллиева мера множества  $A$  равна нулю или это более сильное свойство?

Как и для одиночной вычислимой меры, можно доказать, что существует максимальное эффективно нулевое множество. Для этого достаточно уметь корректировать семейства интервалов так, чтобы после коррекции сумма мер интервалов относительно любой бернуллиевой меры была бы не больше  $\varepsilon$  и чтобы коррекция ничего не меняла, если сумма мер была меньше  $\varepsilon$ . Для этого, получив очередной интервал, мы убеждаемся, что сумма мер интервалов при любом параметре  $p$  меньше  $\varepsilon$  (эта сумма представляет собой многочлен от  $p$  с известными рациональными коэффициентами, и если он всюду меньше  $\varepsilon$ , то в этом можно убедиться).

Теперь можно назвать *бернуллиевыми* те последовательности, которые не содержатся в максимально эффективно нулевом множестве (относительно семейства бернуллиевых мер). Неформально говоря, последовательность  $\omega$  является бернуллиевой, если утверждение о том, что она получена при независимых бросаниях (возможно, несимметричной) монеты не кажется невероятным. А оно будет невероятным, если можно сформулировать некоторое свойство, которое выполняется для  $\omega$ , но является эффективно нулевым относительно класса бернуллиевых мер (и потому для любого значения параметра  $p$  имеет меру нуль и потому невероятно).

Как и для одной меры, это определение можно переформулировать в терминах тестов и дефектов. А именно, будем называть перечислимую снизу функцию  $t$  на бесконечных последовательностях *тестом бернуллиевости*, если её интеграл по любой бернуллиевой мере не превосходит 1. (Вместо единицы можно было бы взять другую константу, но важно, что эта константа не зависит от параметра  $p$ .)

Далее доказывается (как и раньше), что существует максимальный (с точностью до мультиплитивной константы) тест бернуллиевости. Доказательство использует тот факт, что если интеграл данной простой функции по любой бернуллиевой мере меньше 1, то в этом можно убедиться (поскольку интеграл является многочленом от параметра  $p$ ). Логарифм значения этого максимального теста называют *дефектом бернуллиевости*; этот дефект определён с точностью до аддитив-

ной константы.

Как и раньше, бернуллиевость равносильна конечности дефекта. В самом деле, множество тех точек, где универсальный тест больше  $N$ , эффективно открыто и имеет меру не больше  $1/N$  при любом значении параметра. С другой стороны, если при каждом  $\varepsilon$  есть множество интервалов меры меньше  $\varepsilon$ , и  $\chi_\varepsilon$  — характеристическая функция этого множества интервалов, то функция  $\sum 2^n \chi_{4^{-n}}$  будет тестом случайности (с точностью до константы).

## 7 Критерий бернуллиевости

**Теорема.** Последовательность  $\omega$  бернуллиева тогда и только тогда, когда она (релятивизованно) случайна (в смысле Мартин-Лёфа) по бернуллиевой мере  $B_p$  при некотором действительном  $p$  (добавляемым в качестве оракула при определении случайности по Мартин-Лёфу).

Напомним, что определение случайности по Мартин-Лёфу предполагает, что мера вычислима. Поэтому оно не приложимо непосредственно к бернуллиевой мере  $B_p$ , если параметр  $p$  не является вычислимым действительным числом. Но определение Мартин-Лёфа можно релятивизовать, добавив в качестве оракула число  $p$  (например, в форме его двоичного разложения). Такое релятивизованное понятие случайности относительно  $B_p$  уже имеет смысл и именно оно используется в теореме.

**Доказательство** использует понятие *равномерного теста случайности* относительно семейства бернуллиевых мер.

Такой тест представляет собой функцию двух аргументов; неформально говоря,  $t(\omega, p)$  измеряет количество закономерностей в последовательности  $\omega \in \Omega$  относительно меры  $B_p$  для данного  $p \in [0, 1]$ . Мы по-прежнему требуем, чтобы функция  $t$  была перечислена снизу, но теперь определение более сложное, поскольку есть дополнительный параметр  $p$ . А именно, мы требуем, чтобы  $t$  являлась поточечной верхней гранью вычислимой последовательности функций  $t_n$ . Каждая функция  $t_n$  задаётся словом  $z_n$ , рациональным интервалом  $(u_n, v_n)$  и неотрицательным рациональным значением  $c_n$ . При этом  $t_n(\omega, p)$  равно  $c_n$ , если  $\omega$  начинается на  $z_n$ , а  $p$  попадает в интервал  $(u_n, v_n)$ ; в остальных случаях  $t_n(\omega, p) = 0$ .

Вычислимость понимается как существование алгоритма, вычисляющего  $c_n, u_n, v_n, z_n$  по  $n$ . За-

метим ещё, что в число интервалов попадают и полуинтервалы  $[0, v)$  и  $(u, 1]$  (они возникают, если один из краёв интервала  $(u, v)$  выходит за пределы отрезка  $[0, 1]$ ).

Помимо перечислимости снизу, требуется, чтобы при любом  $p \in [0, 1]$  математическое ожидание (то есть интеграл  $t(\omega, p)$  по мере  $B_p$ ) не превосходило единицы.

Далее план доказательства такой:

(1) среди всех равномерных тестов случайности относительно класса бернульиевых мер существует универсальный тест  $u$  (наибольший с точностью до мультипликативной константы);

(2) при этом функция  $u'(\omega) = \inf_p u(\omega, p)$  совпадает с определённым выше универсальным тестом бернульиевости; отсюда видно, что бернульиевость  $\omega$ , то есть конечность  $u'(\omega)$ , равносильна конечности  $u(\omega, p)$  хотя бы для одного  $p \in [0, 1]$ ;

(3) наконец, при данном  $p$  функция  $u_p(\omega) = u(\omega, p)$  совпадает с универсальным тестом случайности относительно меры  $B_p$  (релятивизированным относительно  $p$ ) и потому конечность  $u(\omega, p)$  равносильна (релятивизированной) случайности  $\omega$  по мере  $B_p$ .

Удивительно, но все эти утверждения доказываются без большого труда и новых идей.

(1) Мы можем порождать все перечислимые снизу функции; их надо корректировать, чтобы все математические ожидания были бы не больше 2 и чтобы тесты случайности при коррекции не менялись. В самом деле, на конечном шаге (когда функция есть максимум конечного числа функций  $t_n$ ) математическое ожидание можно вычислить, разбив отрезок  $[0, 1]$  на конечное число промежутков, на каждом промежутке интеграл будет многочленом от  $p$ , и если при каждом  $p$  это меньше 2, то в этом можно убедиться). Только убедившись в этом, мы вводим в употребление очередную функцию  $t_n$ .

Далее складываем скорректированные функции с коэффициентами, сумма которых меньше  $1/2$ .

(2) Рассмотрим функцию  $\inf_p u(\omega, p)$ , где  $u$  — универсальный равномерный тест случайности относительно семейства бернульиевых мер. Нам надо доказать, что она является универсальным тестом бернульиевости. Интеграл этой функции по любой мере  $B_p$  не больше единицы, так как эта функция не превосходит  $t_p$ . Проверим, что она перечислима снизу. Для этого надо установить, что при любом рациональном  $r$  множество последова-

тельностей  $\omega$ , при которых

$$\inf_p u(\omega, p) > r,$$

эффективно открыто (и его можно получать эффективно по  $r$ ). Указанное условие можно переписать так: существует такое  $r' > r$ , что при всех  $p$  значение  $u(\omega, p)$  больше  $r'$ . Условие  $u(\omega, p) > r'$  даёт открытое множество в произведении  $\Omega \times [0, 1]$ , и мы можем перечислять составляющие его интервалы (произведения конусов в  $\Omega$  и интервалов в  $[0, 1]$ ). Интересующее нас свойство состоит в том, что это открытое множество целиком содержит отрезок  $\{\omega\} \times [0, 1]$ . В силу компактности это обстоятельство выясняется на конечном шаге, и потому указанное свойство последовательности  $\omega$  тоже будет эффективно открытым. Квантор существования по  $r'$  (объединение по всем  $r' > r$ ) не нарушает эффективной открытости.

Таким образом, функция  $\inf_p u(\omega, p)$  будет тестом бернульиевости и потому не превосходит максимального такого теста. С другой стороны, любой тест бернульиевости можно рассматривать как равномерный тест, не зависящий от  $p$ , так что выполнено и обратное неравенство.

(3) Пусть сначала  $p$  является вычислимым действительным числом. Тогда функция  $u_p: \omega \mapsto t(\omega, p)$  является перечислимой снизу (для вычислимого действительного числа можно перечислять рациональные интервалы, его содержащие, и тем самым мы можем представить  $u_p$  в виде точной верхней грани вычислимой последовательности простых функций). Поэтому  $u_p$  является тестом случайности по мере  $B_p$ . Таким образом, последовательность, для которой  $u(\omega, p) = \infty$ , не случайна по мере  $B_p$ .

Это же рассуждение можно провести и с оракулом. Взяв в качестве оракула двоичное разложение  $p$ , убеждаемся, что если  $u(\omega, p) = \infty$ , то  $\omega$  не случайна (в  $p$ -релятивизированном смысле) относительно меры  $B_p$ .

Несколько сложнее проверить обратное утверждение. Надо показать, что если  $t$  — перечислимый снизу относительно  $p$  тест случайности по мере  $B_p$  и  $t(\omega) = \infty$ , то можно построить равномерный дефект случайности  $t'$  (перечислимый снизу уже безо всякого оракула), для которого  $t'(\omega, p) = \infty$ .

Для начала рассмотрим случай, когда  $p$  вычислимо и потому  $t$  перечислим снизу. Функцию  $t$  (к которой добавлен фиктивный параметр  $p$ ) нельзя рассматривать как равномерный тест, поскольку

её математическое ожидание по мере  $B_q$  (при  $q \neq p$ ) может быть произвольным. Но её можно пытаться переделать в  $t'$ , которая уже по-настоящему зависит от  $p$ . А именно, перечисляя снизу приближения к  $t$ , мы смотрим, при каких  $q$  происходят нарушения условия на математическое ожидание, и для этих “плохих”  $q$  увеличения не производим (добавляя ограничивающий интервал в перечисление снизу для функции  $t'$ ). При этом оценки можно выполнять с погрешностью, достаточно, чтобы интеграл от  $t'(\omega, q)$  по мере  $B_q$  не превосходил (скажем) 2, и чтобы для тех  $q$ , при которых интеграл от  $t$  был изначально не больше 1, ничего не менялось.

Теперь перейдём к случаю невычислимого  $p$ . В этом случае  $p$  заведомо не будет двоично-рациональным, и потому можно получать биты его разложения, умеля находить сколь угодно точные приближения к  $p$ . Поэтому оракульную машину, перечисляющую снизу  $t$ , если ей дать оракул для  $p$ , можно переделать в перечисление снизу некоторой функции  $\tilde{t}(\omega, q)$ , которая совпадает с  $t$  при  $q = p$ . Эта функция не обязана быть тестом случайности (кроме как при  $q = p$ ), но её можно подвергнуть коррекции. Заметим, что при этой коррекции мы не знаем  $p$ , но и не используем его — мы следим, чтобы коррекция влияла лишь на те  $q$ , при которых интеграл больше 1, и это гарантирует невмешательство при  $q = p$ . Одновременно мы обеспечиваем превышение интеграла (при любом  $q$ ) не более чем в два раза.

[Вопрос. Можно ли определить бернуллиевы последовательности так: берём последовательность независимых равномерно распределённых случайных чисел в  $[0, 1]$  и некоторое число  $p$  (не обязательно вычислимое); далее заменяем числа, меньшие  $q$ , на единицы, а остальные на нули.]

## 8 Равномерные тесты случайности

Идея равномерного теста случайности, применённая выше к классу бернуллиевых мер, может быть применена и к классу всех мер на пространстве  $\Omega$ . В этом случае в качестве тестов случайности надо рассматривать функции  $t(\omega, P)$  с двумя аргументами: первый является последовательностью из  $\omega$ , а второй — мерой на  $\Omega$ . (Значения функций неотрицательны, допускается и  $+\infty$ .) При этом ограничение на математическое ожидание ясно: мы тре-

буем, чтобы при любом  $P$  интеграл от функции  $\omega \mapsto t(\omega, P)$  по мере  $P$  не превосходил 1. Осталось определить перечислимость снизу.

Будем называть *интервалом* в пространстве мер множество мер, которое задаётся набором условий вида  $r_1 < P(u) < r_2$ , где  $u$  — некоторое двоичное слово, а  $r_1, r_2$  — рациональные числа. *Простой функцией* называется функция  $t(\omega, P)$ , которая равна некоторой рациональной константе, когда  $\omega$  начинается на данное слово, а  $P$  принадлежитциальному интервалу в пространстве мер, и равна нулю в противном случае. Такие функции имеют естественную нумерацию. *Перечислимой снизу* функцией называем точную верхнюю грань вычислимой последовательности простых функций.

Как обычно, среди всевозможных тестов случайности существует максимальный с точностью до константы. В самом деле, обычное построение требует умения корректировать перечислимую снизу функцию, чтобы она становилась тестом (почти тестом) и не менялась, если уже была тестом. Для максимума конечного числа простых функций это обстоятельство можно проверить (интеграл является линейной функцией от мер конечного числа слов на участках, задаваемых наборами линейных неравенств, и соответствующие проверки легко выполнить).

Максимальный тест случайности  $u(\omega, P)$  можно затем использовать для определения случайности по произвольной мере (не обязательно вычислимой), объявив последовательность  $\omega$  случайной по мере  $P$ , если  $u(\omega, P) < \infty$ .

Во что превращается это определение, если мера вычислена? Для вычислимой меры  $P$  функция  $\omega \mapsto u(\omega, P)$  является перечислимой снизу, поскольку можно перечислять все интервалы, содержащие меру  $P$ . Поэтому эта функция является тестом случайности (в старом смысле слова) относительно меры  $P$ . Поэтому если  $u(\omega, P) = \infty$ , то  $\omega$  не случайна по Мартин-Лёфу относительно меры  $P$ .

Покажем, что верно и обратное. Пусть имеется некоторая перечислимая снизу функция  $t$  на  $\omega$ , являющаяся тестом случайности относительно меры  $P$ . Функция  $\tilde{t}(\omega, Q) = t(\omega)$  не будет равномерным тестом случайности, поскольку её интеграл при  $Q \neq P$  может быть произвольным. Однако её можно корректировать. В самом деле, для конечного числа слов, появившихся в приближении снизу к функции функции  $t$ , интеграл по мере  $P$  определяется конечным числом значений меры

на словах. Условие “интеграл не больше 1” задаёт в соответствующем конечномерном пространстве некоторый многогранник, который можно приблизить объединением интервалов в пространстве мер. Взяв приближение достаточно точным, мы не изменим функцию там, где интеграл был меньше единицы, но добьёмся, чтобы он везде не превосходил 2.

Следовательно, из неслучайности по Мартин-Лёфу относительно  $P$  следует неслучайность в новом смысле.

Аналогичное утверждение верно и в случае, когда если мера вычислима относительно некоторого оракула  $A$  и сам оракул  $A$  можно восстановить, умея вычислять значения меры с произвольной точностью. В этом случае определение случайности с помощью равномерных тестов совпадает с определением Мартин-Лёфа, релятивизованным относительно  $A$ . В самом деле, если  $t$  является равномерным тестом случайности, а  $P$  — вычислимая относительно  $A$  мера, то функция  $\omega \mapsto t(\omega, P)$  является перечислимой снизу относительно  $A$  и представляет собой (релятивизованный относительно  $A$ ) тест случайности относительно меры  $P$ .

С другой стороны, если имеется перечислимый снизу относительно  $A$  тест относительно  $P$ , то можно построить перечислимую снизу функцию двух аргументов, которая совпадает с этим тестом, если второй аргумент положить равным  $P$ . (Здесь используется тот факт, что множество  $A$  можно восстановить, умея вычислять значения меры  $P$  с произвольной точностью.) Эта функция не будет тестом, так как условие на интеграл выполнено, лишь если второй аргумент равен  $P$ . Но её можно сделать тестом, подвергнув коррекции, после которой интеграл при любой мере не превосходит 2, и значения остались прежними в том случае, когда интеграл и так был не больше 1.

Доказанный результат делает ещё более удивительной следующую теорему (которая есть в заметках Гача): существует мера, относительно которой любая последовательность случайна. Ведь для любой вычислимой меры существует не случайная относительно этой меры последовательность (выбираем очередной член так, чтобы вероятность интервала уменьшилась по крайней мере в полтора раза; получаем вычислимую последовательность, которая имеет меру нуль). Это же верно и с любым оракулом. Поэтому мера, относительно которой любая последовательность случайна, не экви-

валентна никакому оракулу (не существует оракула, относительно которого она вычислима и который может быть восстановлен по приближениям к мере).

Можно ли считать это определение случайности относительно произвольной меры интуитивно удовлетворительным? Недостаток: пусть последовательность случайна относительно меры  $P$  и начинается на нуль. Изменим значения меры на последовательностях, начинающихся на единицу (или даже на несколько единиц подряд). При этом определение случайности может измениться, если теперь мера является более сильным оракулом (позволяет вычислять что-то, что раньше не было вычислимым). По аналогичным причинам случайность по мере, которая получается из равномерной добавлением чего-нибудь очень малого, но плохо вычислимого, отличается от случайности по равномерной мере. (Что кажется противоречащим нашей интуиции.)

[Что можно сказать о таком варианте определения: берём последовательность независимых случайных чисел в  $[0, 1]$  (в смысле Мартин-Лёфа) и затем сравниваем очередное число с требуемой мерой условной вероятностью появления единицы?]