

Л. А. ЛЕВИН

О ПРИНЦИПЕ СОХРАНЕНИЯ ИНФОРМАЦИИ В ИНТУИЦИОНИСТСКОЙ МАТЕМАТИКЕ

(Представлено академиком А. Н. Колмогоровым 12 I 1976)

1. Рассматривается одна новая интуиционистская аксиоматическая теория, основанная на принципе сохранения информации (аксиомная схема (4,1)). Этот принцип утверждает, что в процессе свободного становления последовательности не может неограниченно возрастать количество содержащейся в ней нетривиальной информации об истинности арифметических предикатов. При этом используется понятие «количества информации», введенное А. Н. Колмогоровым ⁽²⁾ на базе понятия «алгоритмической сложности» и затем уточненное в ⁽³⁾. В ⁽³⁾ был также изучен «принцип сохранения информации» в форме законов теории вероятностей и сформулирован тезис I, согласно которому такие законы выполняются в любых вообще процессах произвольной физической природы. Если интерпретировать интуиционистские последовательности как последовательности, члены которых могут быть получены в каком-нибудь процессе, реально происходящем в физическом мире, то указанный тезис обосновывает естественность принятия принципа (4,1).

Если называть «элементарным» физический процесс, порождающий последовательность, которую нельзя представить как результат применения вычислимого оператора к результату физического процесса «более простого», чем исходный, то, экстраполируя свойства известных явлений природы, правдоподобно предположить, что:

1) любой процесс в природе, порождающий последовательность, можно «понять», т. е. представить в виде суперпозиции «элементарного» (в указанном выше смысле) физического процесса и вычислимого оператора;

2) последовательность, порождаемая элементарным физическим процессом, всегда случайна по какому-нибудь очень простому распределению вероятностей.

Тогда теорем работы ⁽³⁾ о невозрастании информации в случайных и вычислимых процессах достаточно для обоснования принципа сохранения информации.

2. Новая теория $\mathcal{A}$ Inf будет построена путем добавления ряда аксиом ((4,1), (4,2) и $\neg$ (5,1)) к исчислению $\mathcal{A}$, которое мы опишем в этом пункте и примем за основу. $\mathcal{A}$ формулируется в обычном языке арифметики второго порядка. Этот язык получается добавлением к языку арифметики I порядка (см. ⁽¹⁾, § 38) счетного списка переменных второго порядка, означающих последовательности натуральных чисел или функции, а также следующих правил образования термов и формул: если α — переменная второго порядка, t — терм, а Φ — формула, то $\alpha(t)$ — терм, а $\forall \alpha \Phi$ и $\exists \alpha \Phi$ — формулы. Абсолютной будем называть формулу, построенную из равенств между термами при помощи конъюнкции, отрицания и квантора общности по переменным первого порядка. Абсолютные формулы имеют одинаковый смысл в интуиционистских и классических теориях. Под парой термов (a_1, a_2) будем подразумевать терм $(a_1 + a_2)^2 + a_1$. Очевидно, что эта нумерация пар обратима. В таком же смысле будем понимать выражения $(a_1, \dots, a_n)$; $\alpha(a_1, \dots, a_n)$; (α, β) и пр. Пусть для числа n и терма α верна $\exists t_0 (\alpha(t_0) = n + 1 \ \& \ \forall t < t_0 \ \alpha(t) = 0)$. Тогда, допуская воль-

ность речи, мы будем применять следующее обозначение этого факта: $n = \text{pr}_t \alpha$ (n равно проекции по t терма α). Обращение с выражением $\text{pr}_t \alpha$ как с термом нигде не вызовет недоразумений, в частности, благодаря (2,2). Аксиомы $\mathcal{A}$ состоят из аксиом арифметики первого порядка (см. (1^a), стр. 467, схема 8 берется в интуиционистском варианте 8') и следующих трех принципов арифметики 2-го порядка:

Схема выбора:

$$(\forall n (\neg A \rightarrow \exists x P(x))) \rightarrow \exists \alpha \forall n (\neg A \rightarrow P(\text{pr}_t \alpha(n, t))); \quad (2,1)$$

Ленинградский принцип:

$$\forall \alpha ((\neg \forall n \alpha(n) = 0) \rightarrow \exists n \alpha(n) \neq 0); \quad (2,2)$$

Аксиома счетности:

$$\exists \alpha \forall \beta \exists k \forall n \beta(n) = \text{pr}_t \alpha(k, n, t). \quad (2,3)$$

(2,3) утверждает, что множество интуиционистских последовательностей счетно. При интерпретации интуиционистских последовательностей, как последовательностей результатов реальных макрособытий физического мира, аксиома (2,3) соответствует довольно привычному утверждению о сепарабельности пространства-времени. Мы не будем подробно обсуждать аксиомы $\mathcal{A}$, так как это многократно делалось в литературе. Отметим только, что для построения любого «законченного» (удовлетворяющего теореме 1) исчисления необходимо принять или эти аксиомы (хотя бы под двойным отрицанием), или их отрицания, или их эквивалентность каким-нибудь неразрешимым абсолютным утверждениям теории чисел. Последние два варианта кажутся нам менее естественными. Хорошо известно, что (2,1) — (2,3) несовместимы с принципами непрерывности и Ваг-индукции. Этим исчисление $\mathcal{A}$ больше напоминает конструктивный анализ. Однако принципиальная разница между ними состоит в отсутствии в $\mathcal{A}$ тезиса Чёрча. Отказ от него диктуется желанием интерпретировать последовательности нашей теории, как последовательности результатов событий, происходящих в природе. Конечно же исчисление $\mathcal{A}$, лишенное и Ваг-индукции и тезиса Чёрча, является еще слишком слабым. Однако все же справедливо

Предложение 1. *Для всякой формулы Φ существует абсолютная формула P такая, что $\mathcal{A} \vdash \Phi \leftrightarrow \forall \alpha \exists \beta P$.*

3. Некоторые понятия алгоритмической теории информации. Вспомогательные сведения этого пункта изложены кратко и поверхностно. Подробнее см. в (3) (а также в (2, 5)).

Неотрицательную действительную функцию $f(x)$, определенную на конечных наборах натуральных чисел, будем называть *перечислимой* (снизу), если перечислимо множество пар (r, x) таких, что r — рациональное число, меньшее $f(x)$. Функцию $f(x, \alpha)$ назовем *перечислимой* (снизу), если $f(x, \alpha) = \sup f'(x, (\alpha)_n)$, где x — натуральное число, α — бесконечная последовательность натуральных чисел, $(\alpha)_n$ — ее начальный фрагмент длины n , а f' — перечислимая функция. Функция $f(x)$ будет *вычислимой*, если перечислимы функции $f(x)$ и $1/f(x)$. Знаки $\geq$, $\leq$, $\times$ означают неравенства и равенства с точностью до аддитивной константы.

Предложение 2. *Существуют максимальные с точностью до мультипликативной константы полувычислимые функции в классах: а) $\{f: \sum f(x) < \infty\}$; б) $\{f: \forall \alpha \sum f(x, \alpha) < \infty\}$; в) $\{f: \forall s \sum f(sx) \leq f(s)\}$, где x — натуральное число, α — последовательность, sx — последовательность, полученная приписыванием x к конечной последовательности s .*

Первую из этих максимальных функций обозначим $P(x)$, вторую — $P(x|\alpha)$, третью — $M(s)$; целые части модулей их логарифмов обозначим соответственно $KP(x)$, $KP(x|\alpha)$ и $KM(s)$. Пусть α, β — конечные или бесконечные последовательности. Тогда количеством информации в каждой

из них о другой назовем величину

$$I(\alpha:\beta) = \left[\log_2 \sum (P(x|\alpha) \cdot P(y|\beta) \cdot P(x,y)/P(x) \cdot P(y)) \right].$$

Для конечных s и любых β справедливо $KM(s) \geq I(s:\beta)$, поэтому $KM(s)$ может служить характеристикой «полного количества информации в s », или «сложности s ». Пусть $f(s)$ — произвольная вычислимая функция такая, что $f(s) \geq \sum f(sx)$. Тогда $[-\log_2 f(s)] \geq KM(s)$ по определению KM . Для некоторых α может существовать такая вычислимая f , для которой это неравенство становится равенством $KM((\alpha)_n) \asymp [-\log_2 f((\alpha)_n)]$. Тогда с помощью f можно эффективно вычислять $KM((\alpha)_n)$ с точностью до аддитивной константы для всех n (а вообще KM невычислима). Такие последовательности α называются полными. Таким образом, полные последовательности содержат всю информацию о сложности своих фрагментов, достаточную для ее вычисления. Множество полных последовательностей замкнуто относительно вычислимых всюду определенных операторов; любая вычислимая мера его дополнения равна нулю. Термин «полнота», в частности, оправдывается тем, что любую последовательность можно «пополнить» без использования какой-либо «запретной» информации, точнее имеет место

Предложение 3. Пусть β — последовательность, к которой сводимо универсальное перечислимое множество, α — последовательность такая, что $I(\alpha:\beta) < \infty$.

Тогда существует γ такая, что пара (γ, α) полна и $I((\gamma, \alpha):\beta) < \infty$.

4. Информационное исчисление $\mathcal{A} \text{ Inf}$. Пусть $\mathcal{P}(n)$ — абсолютный предикат с единственной свободной переменной n . Конечную двоичную последовательность p длины k будем называть согласованной с $\mathcal{P}$, если при любом $n \leq k$ n -й знак p равен 0 тогда и только тогда, когда справедливо $\mathcal{P}(n)$ (обозначать этот факт мы будем $p \subset \mathcal{P}$). Под сокращением $I(\alpha:\mathcal{P})$ мы будем подразумевать $\sup I(\alpha:p): p \subset \mathcal{P}$. Очевидно, что утверждение $I(\alpha:\mathcal{P}) \leq c$ можно при каждом конкретном $\mathcal{P}$ записать в виде абсолютного предиката со свободными переменными α и c .

Принцип сохранения информации является схемой аксиом ($\mathcal{P}$ — параметр этой схемы). В принятых выше сокращениях этот принцип записывается так:

$$\forall \alpha \exists c \quad I(\alpha:\mathcal{P}) \leq c. \quad (4,1)$$

В $\mathcal{A} \text{ Inf}$ должно быть справедливо еще одно утверждение, связанное с теорией информации. Мы его введем ниже в качестве последней аксиомы теории, однако мы не умеем доказывать независимость этой аксиомы (может оказаться, что ее двойное отрицание является следствием предыдущих аксиом). В п. 3 определяется понятие «полной» последовательности. Свойство «быть полной» выразимо абсолютным предикатом $\Pi(\alpha)$. Наша последняя аксиома требует, чтобы для последовательностей нашей теории пополнение из предложения 3 существовало в рамках этой теории:

$$\forall \alpha \exists \gamma \quad \Pi(\alpha, \gamma). \quad (4,2)$$

Двойное отрицание этой аксиомы вытекает из более слабого утверждения $\neg \exists \alpha \forall \gamma \neg \Pi(\alpha, \gamma)$, поскольку мы можем использовать существование «универсальной» последовательности из аксиомы (2,3). Аналогично двойное отрицание принципа (4,1) вытекает из утверждения $\neg \exists \alpha \forall c \quad I(\alpha:\mathcal{P}) \geq c$. Для наших целей было бы достаточно ограничиться этими более слабыми вариантами аксиом, но мы выбрали формулировки (4,1) и (4,2), так как они проще.

5. Абсолютность. Непротиворечивость и полнота относительно классической арифметики.

Определение. Мы будем говорить, что теория G абсолютна, если для всякой замкнутой формулы Φ найдется абсолютная (см. п. 2) формула P такая, что $G \vdash \neg \neg (\Phi \leftrightarrow P)$.

Примером известной абсолютной теории является конструктивный анализ. Это теория, получающаяся из $\mathcal{A}$ заменой (2,3) на тезис Чёрча (т.Ч.):

$$\forall \beta \exists k \forall n \quad \beta(n) = u(k, n), \quad (5.1)$$

где $u(k, n)$ — универсальная частично рекурсивная функция. ((5.1) получается из (2,3) наложением условия общерекурсивности на α .) Наша теория $\mathcal{A} \text{ Inf}$, конечно же, не абсолютна, поскольку формула $\neg\neg$ (т.Ч.) в ней не выводима, не опровержима и не сводима ни к какой абсолютной. Однако указанная формула является единственной в этом роде, а именно справедлива

Основная лемма. Для любой замкнутой формулы Φ существует четыре абсолютные формулы P_1, P_2, P_3, P_4 такие, что в $\mathcal{A} \text{ Inf}$ выводимы утверждения:

$$\neg\neg(P_1 \vee P_2 \vee P_3 \vee P_4); \quad \neg\neg(P_1 \supset \Phi); \quad \neg\neg(P_2 \supset \neg\Phi); \\ \neg\neg(P_3 \supset (\Phi \supset (\Phi \supset (\text{т.Ч.})))); \quad \neg\neg(P_4 \supset (\Phi \supset \neg(\text{т.Ч.}))).$$

Для получения «законченной» теории необходимо принять аксиому, влекущую истинность или ложность (т.Ч.). Оказывается, что этого и достаточно. Теория $\mathcal{A} \text{ Inf} + (\text{т.Ч.})$ эквивалентна конструктивному анализу и, следовательно, абсолютна. Она мало интересна для наших целей, поскольку принятием тезиса Чёрча мы исключаем из рассмотрения последовательности, не задаваемые алгоритмами (например, случайные). В той мере, в которой (т.Ч.) является очень сильной аксиомой, аксиома $\neg$ (т.Ч.) является, наоборот, очень слабой. Тем неожиданнее, что теория $\mathcal{A} \text{ Inf} + \neg$ (т.Ч.) также абсолютна. Этот факт вытекает из основной леммы и усиливается в следующей теореме.

Теорема 1. Класс абсолютных замкнутых формул, выводимых в $\mathcal{A} \text{ Inf} + \neg$ (т.Ч.), совпадает с классом абсолютных теорем классической арифметики (первого порядка). Никакое существенное (т. е. содержащее новые теоремы вида $\neg\neg\Phi$) расширение теории $\mathcal{A} \text{ Inf} + \neg$ (т.Ч.) этим свойством не обладает.

Таким образом, теория $\mathcal{A} \text{ Inf} + \neg$ (т.Ч.) является в определенном смысле законченной и обладает свойством, которое можно назвать непротиворечивостью и полнотой относительно классической арифметики. Основной целью построения этой теории было рассмотрение аксиомной схемы (4.1). Мы желали продемонстрировать силу этой схемы, дополнив ее до теории, удовлетворяющей теореме 1. Не исключено, что такое дополнение можно сделать и другими естественными способами. Мы выбрали его, следуя аналогии с обычной аксиоматикой конструктивного анализа.

На настоящую статью оказали благотворное влияние несколько обсуждений на семинаре чл.-корр. АН СССР А. А. Маркова в 1969 — 1973 гг., на симпозиуме по основаниям математики (Обнинск, 1971 г.), на семинаре А. Г. Драгалина и в других местах. Автор выражает глубокую благодарность всем участникам обсуждений. Автор благодарен Г. Гаргову за библиографические указания.

Поступило
7 VII 1975.

ЛИТЕРАТУРА

- ¹ S. C. Kleene, Mathematical Logic, N. Y., 1967; а) Русск. пер. С. К. Клини, Математическая логика, М., «Мир», 1973. ² А. Н. Колмогоров, Проблемы передачи информации, т. 1, № 1, 3 (1965). ³ Л. А. Левин, Проблемы передачи информации, т. 10, № 3 (1974). ⁴ S. C. Kleene, R. E. Vesley, The Foundations of Intuitionistic Mathematics Especially in Relation to Recursive Functions, Amsterdam, 1965. ⁵ Л. А. Левин, ДАН, т. 227, № 4 (1976). ⁶ G. Kreisel, A. S. Troelstra, Ann. Math. Logic, v. 1, № 3, 229 (1970).