PDMI Preprint 09/2022

Индуктивные и коиндуктивные конструкции в математике

Н. В. Дуров[1]

[1] Санкт-Петербургское отделение Математического института им. В. А. Стеклова Российской Академии Наук

email: douroff@pdmi.ras.ru

Аннотация. Данная работа продолжает обсуждение абсолютной геометрии и возможных подходов к её построению, начатое в [AB1]. Вероятностные конструкции из [AB1] подсказывают, что искомая «абсолютная база» $\mathcal{B}$ может быть очень большим объектом. В связи с этим имеет смысл обсудить, какие именно конструкции могут быть полезны для построения такого рода больших объектов. В настоящей работе мы сосредотачиваем внимание на индуктивных и коиндуктивных конструкциях в математике и показываем, как они могут быть применены, в частности, для формализации вероятностных конструкций из [AB1].

Ключевые слова: Абсолютная геометрия, поле из одного элемента, индуктивные конструкции, коиндуктивные конструкции.

ПРЕПРИНТЫ ПОМИ РАН

Учредитель: Федеральное государственное бюджетное учреждение науки
Санкт-Петербургское отделение Математического института
им. В. А. Стеклова Российской академии наук

Свидетельство о регистрации средства массовой информации:
ЭЛ № ФС 77-33560 от 16 октября 2008 г.
Выдано Федеральной службой по надзору
в сфере связи и массовых коммуникаций

Контактные данные:

191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27

телефоны: (812) 312-40-58; (812) 571-57-54

e-mail: admin@pdmi.ras.ru

http://www.pdmi.ras.ru/preprint/

Заведующая информационно-издательским сектором В. Н. Симонова

3 Индуктивные и коиндуктивные конструкции в математике

Мы видели, что «правильная» абсолютная база $\mathcal{B}$, т.е. база для абсолютной геометрии, может быть большим объектом, например, «бесконечномерным симплексом» $\Delta([0,1])$ из [AB1],**2.1.19**, и что, возможно, именно поэтому правильная конструкция абсолютной геометрии ускользает от нас. Такого рода объекты, обычно представляющие из себя множества мощности континуум с некоторой естественной топологией, обычны в анализе и смежных областях математики, однако представляются менее естественными с точки зрения алгебры. Поэтому мы должны понять, как соотносятся «алгебраические» и «аналитические» объекты, и насколько естественно они могут смешиваться.

3.1 Индуктивные и коиндуктивные конструкции

Одним из способов формального определения и различения «алгебраических» и «аналитических» объектов являются индуктивные и коиндуктивные конструкции, см. [CH1], [CH2], [CP].

3.1.1. (Индуктивные и коиндуктивные конструкции в категории множеств, в топосах и в произвольных категориях.) Отметим, что индуктивные и коиндуктивные конструкции наиболее естественно возникают в интуиционистской теории зависимых типов Мартин–Лёфа, моделями которой являются топосы. Поэтому естественно рассматривать эти конструкции в топосах. Однако многие конкретные конструкции могут быть рассмотрены в более общих категориях $\mathcal{C}$, например, декартовых или декартово-замкнутых. Так, мы будем применять некоторые конструкции не только в $\mathcal{C} = \mathit{Sets}$, но и в категориях топологических или равномерных пространств, которые не являются топосами. С другой стороны, в «обычной математике» все эти конструкции обычно применяются только в категории множеств, где они наиболее наглядны или как минимум привычны.

Все эти конструкции естественным образом распространяются на гомотопическую теорию типов, моделями которой должны быть ∞-топосы в смысле J. Lurie, однако это утверждение пока не доказано строго. Тем не менее, отметим, что при желании можно было бы использовать ∞-топосы или более общие ∞-категории в качестве $\mathcal{C}$.

3.1.2. (Таблица сравнения индуктивных и коиндуктивных конструкций.) Прежде, чем обсуждать формальные определения, приведем сводную таблицу, где сравниваются индуктивные и коиндуктивные конструкции, чтобы дать неформальное представление о предмете.

конструкции	индуктивные	коиндуктивные
типичные примеры	$\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\bar{\mathbb{Q}}$	отрезок $[0,1]$, $\mathbb{R}$, $\mathbb{C}$, $L^2(\mathbb{R})$, $\mathbb{Z}_p$
примеры конструкций	многочлены $K[x]$	формальные ряды $K[[x]]$
	конечные слова (списки) A^* над алфавитом A	бесконечные последовательности A^ω
типичные элементы	конструктивные (формулы, выражения)	пределы последовательностей
естественная топология	обычно дискретная	недискретная
полнота	нет	часто да
мощность множества	конечное или счетное	континуум
универсальное свойство	инициальный объект	финальный объект
свойство подъема	левое свойства подъема	правое свойство подъема
гомологическая алгебра	свободные или проективные резольвенты	инъективные резольвенты
гомотопическая алгебра	корасслоенные объекты	расслоенные объекты
гомотопические типы	симплициальные множества	топологические пространства

3.1.3. (Пример индуктивной конструкции: натуральные числа.) Самым главным примером индуктивной конструкции являются натуральные числа $\mathbb{N}_0$. Напомним, согласно аксиомам Пеано натуральные числа могут быть охарактеризованы следующим образом:

- Есть выделенное натуральное число 0. На категорном языке это означает, что дан морфизм $o : 1 \to N$ из финального объекта $1 = 1_{\mathcal{C}}$ данной категории $\mathcal{C}$ в объект натуральных чисел N.
- Для каждого натурального числа n есть следующее, которое мы обозначим n^+ либо $s(n)$. Иначе говоря, дан эндоморфизм $s : N \to N$.
- Каждое натуральное число n есть либо 0, либо $s(m)$ для однозначно определенного натурального числа m (здесь объединены две аксиомы Пеано: $(\forall n)(n^+ \neq 0)$ и $(\forall m)(\forall n)(m^+ = n^+ \Rightarrow m = n)$). На категорном языке это означает, что $(o, s) : 1 \sqcup N \to N$ — изоморфизм, где $1 \sqcup N$ обозначает копроизведение.
- Аксиома индукции: если некоторое подмножество множества натуральных чисел содержит 0, и вместе с каждым натуральным числом n содержит следующее за ним, то оно совпадает со всем множеством натуральных чисел. Иначе говоря, каждое натуральное число может быть построено из нуля путем применения операции s конечное число раз.

Аксиому индукции сложнее всего формализовать, потому что она не выражается в логике первого порядка (нам нужен квантор по подмножествам множества натуральных чисел либо по предикатам, описывающим свойства натуральных чисел). Один из вариантов — с квантором по предикату: $(\forall P : N \to \mathbb{B})(P(0)\&(\forall n : N)(P(n) \Rightarrow P(n^+)) \Rightarrow (\forall n : N)(P(n))$. В рамках теории категорий формализовать такое условие довольно сложно (понадобится как минимум элементарный топос). Лучше заметить, что по существу аксиома индукции означает, что нет «лишних» натуральных чисел, т.е. что множество натуральных чисел настолько мало, настолько это возможно. Это просто означает, что множество или объект натуральных чисел N есть инициальный объект в категории, состоящей из троек $(N, o : 1 \to N, s : N \to N)$, удовлетворяющих остальным аксиомам Пеано.

Это определение объекта натуральных чисел используется, например, в теории элементарных топосов. Если в элементарном топосе есть объект натуральных чисел, то далее оказываются возможными и другие индуктивные конструкции, и элементарный топос оказывается почти топосом Гротендика. Аналогичным образом, в теории множеств существование множества натуральных чисел приходится гарантировать с

помощью отдельной аксиомы, однако после этого становятся возможны более-менее все содержательные математические конструкции.

3.1.4. (Категорное определение объекта натуральных чисел.) Мы только что определили объект натуральных чисел N в произвольной категории $\mathcal{C}$ как инициальный объект в категории троек (N, o, s), где $N : \mathrm{Ob}\,\mathcal{C}$, $o : 1_{\mathcal{C}} \to N$ и $s : N \to N$ таковы, что $(o, s) : 1_{\mathcal{C}} \sqcup N \to N$ — изоморфизм. Отметим, что этими условиями N, вернее, тройка (N, o, s) определяется однозначно с точностью до канонического изоморфизма. Более того, последнее условие, что (o, s) — изоморфизм, обычно избыточно, инициальный объект в категории троек $(N : \mathcal{C}, o : 1 \to N, s : N \to N)$ будет автоматически обладать этим свойством, если копроизведение $1 \sqcup N$ существует в $\mathcal{C}$, поскольку окажется, что $(1 \sqcup N, i_1 : 1 \to 1 \sqcup N, s' : 1 \sqcup N \to 1 \sqcup N)$, где $s' = (i_2 o, i_2 s)$, т.е. $s' i_1 = i_2 o$ и $s' i_2 = i_2 s$, где $i_1 : 1 \to 1 \sqcup N$ и $i_2 : N \to 1 \sqcup N$ обозначают естественные вложения — еще один инициальный объект в этой категории троек, и потому существует изоморфизм $\theta : 1 \sqcup N \xrightarrow{\sim} N$, такой, что $\theta i_1 = o$ и $\theta s' = s\theta$; отсюда легко выводится $\theta = (o, s)$.

Важным во всем этом является то, что объект натуральных чисел оказывается инициальным объектом в некоторой категории конечных диаграмм внутри $\mathcal{C}$.

3.1.5. (Индуктивные конструкции: списки, или конечные слова A^*.) Следующий по сложности пример индуктивной конструкции — это множество конечных слов A^* над данным алфавитом A. Алфавит A может быть конечным или счетным множеством, или каким угодно ранее построенным множеством, или объектом категории $\mathcal{C}$. Иначе говоря, теперь речь идет об индуктивной конструкции или о функторе, который принимает параметр A и изготовляет из него A^*. Сам параметр A при этом может быть, например, построен с помощью другой индуктивной или коиндуктивной конструкции или как-нибудь еще.

Конечные слова A^* могут быть описаны следующим образом:

- [Пустое слово.] Существует пустое слово $\emptyset \in A^*$.
- [Конкатенация.] Если $x \in A$ и $\alpha \in A^*$, то конкатенация $x\alpha$ — тоже слово.
- [Единственность представления.] Любое слово либо пусто, либо однозначно представимо в виде конкатенации $x\alpha$.

- [Структурная индукция.] Все слова получаются из пустого слова с помощью конечного числа применения правила конкатенации. Иначе говоря, если подмножество $P \subset A^*$ содержит $\emptyset$, и вместе с каждым $\alpha \in P$ содержит $x\alpha$ для всех $x \in A$, то $P = A^*$.

Эти аксиомы аналогичны аксиомам Пеано, и в действительности являются их обобщением (если в качестве A взять одноэлементное множество либо финальный объект категории, то аксиомы для A^* станут аксиомами Пеано). Они могут быть категорифицированы следующим образом: A^* — это инициальный объект в категории всех троек $(X : \mathcal{C}, \emptyset : 1_{\mathcal{C}} \to X, c : A \times X \to X)$, где мы предполагаем, что в $\mathcal{C}$ существуют конечные декартовы произведения. Если в $\mathcal{C}$ есть конечные копроизведения, то окажется, что $(\emptyset, c) : 1 \sqcup (A \times X) \to X$ — изоморфизм, поскольку $1 \sqcup (A \times X)$ будет удовлетворять тому же универсальному свойству, что и X, аналогично **3.1.4**, т.е. существование и единственность представления снова являются следствиями универсального свойства.

3.1.6. (Дальнейшие примеры индуктивных конструкций: арифметические выражения, формулы, многочлены, свободные группы, свободные абелевы группы.) Ясно, что аналогичным образом мы можем определить, например, арифметические выражения, логические формулы и т.п. Скажем, арифметическое выражение — это либо целое число, либо одна из переменных из данного фиксированного списка A, либо одно из $(E + E')$, $(E - E')$, $(E \cdot E')$, где E и E' — арифметические выражения. Затем мы можем потребовать существование и единственность такого представления, сформулировать принцип структурной индукции, и переформулировать все это как инициальное свойство в некоторой категории. Если же мы захотим определить многочлены $\mathbb{Z}[A]$ с целыми коэффициентами относительно переменных из A, то мы можем сделать это, например, с помощью подходящего отношения эквивалентности на арифметических выражениях с переменными из A. Надо только проверить, что это отношение эквивалентности «конструктивно» или «индуктивно» в некотором смысле. В действительности вопрос о том, какие именно отношения индуктивны, тоже интересен; мы пока ограничимся тем, что индуктивные отношения задаются конечным набором правил вида «если $x_1 \sim y_1$, …, $x_m \sim y_m$, то $E(x_1, \ldots, x_m) \sim E(y_1, \ldots, y_m)$», где E — некоторое допустимое выражение со свободными переменными. При этом $\sim$ — это *наименьшее* отношение, удовлетворяющее данному набору правил. Такого рода отношения часто возникают в логике и в алгебре.

Тем самым мы видим, что почти все конструкции в алгебре и логике являются индуктивными.

3.1.7. (Пример коиндуктивной конструкции: отрезок $I = [0, 1]$.) Коиндуктивные конструкции определяются аналогично индуктивным, однако теперь в некоторой категории конечных диаграмм внутри данной категории $\mathcal{C}$ мы берем не инициальный, а финальный объект. Он снова будет однозначно определен с точностью до канонического изоморфизма. Однако свойства коиндуктивных объектов обычно совсем не такие, как у индуктивных. В качестве примера рассмотрим коиндуктивное определение отрезка $I = [0, 1]$:

- Есть два выделенных элемента $0, 1 \in I$ (на категорном языке — два морфизма l, $r : 1_{\mathcal{C}} \to I$), и при этом $0 \neq 1$ (на категорном языке — расслоенное произведение $1_{\mathcal{C}} \times_{l,r} 1_{\mathcal{C}}$ есть инициальный объект $\varnothing$).
- Существует изоморфизм $\theta : I \xrightarrow{\sim} I \sqcup_{r,l} I$, такой, что $\theta l = i_1 l$ и $\theta r = i_2 r$, где $I \sqcup_{r,l} I$ означает пушаут

$$\begin{array}{ccc} 1 & \xrightarrow{l} & I \\ \downarrow{\scriptstyle r} & & \downarrow \\ I & \longrightarrow & I \sqcup_{r,l} I \end{array} \tag{3.1.7.1}$$

- (I, l, r, θ) — финальный объект среди всех таких четверок.

Фактически здесь сказано, что любой элемент $I = [0, 1]$ есть либо $x/2$, либо $(x+1)/2$ для некоторого $x \in I$, причем все эти элементы различны, за исключением случая $1/2 = (0 + 1)/2$. При этом мы должны взять «самый большой» такой I, иначе, например, двоично-рациональные или рациональные числа из отрезка $[0, 1]$ также будут удовлетворять этим аксиомам. Как и для индуктивных конструкций, достаточно требовать существование морфизма $\theta : I \to I \sqcup_{r,l} I$, его изоморфность является следствием универсального свойства (I, l, r, θ).

3.1.8. (Пример коиндуктивной конструкции: бесконечные последовательности $A^\omega = A^{\mathbb{N}}$ над алфавитом A.) Другой характерный пример коиндуктивной конструкции — это множество (или объект) A^ω бесконечных последовательностей над фиксированным алфавитом A (который может быть произвольным объектом данной категории $\mathcal{C}$). В этом случае мы требуем следующее:

- Любой элемент $X = A^\omega$ есть конкатенация $x\alpha$, где $x \in A$, $\alpha \in A^*$. Иначе говоря, дан (изо)морфизм $\theta : X \to A \times X$.
- (X, θ) — финальный объект в категории всех пар $(X : \mathcal{C}, \theta : X \to A \times X)$.

Снова изоморфность θ следует из универсального свойства (X, θ), поскольку $(A \times X, \mathrm{id}_A \times \theta)$ обладает тем же универсальным свойством.

3.1.9. (Вариант: конечные и бесконечные последовательности вместе.) При желании мы можем сделать предыдущий пример чуть более похожим на **3.1.5**, разрешив последовательностям обрываться после конечного числа элементов. В этом случае надо рассматривать структурный (изо)морфизм $\theta : X \to 1_{\mathcal{C}} \sqcup (A \times X)$, который будет означать, что любой элемент X есть либо пустая последовательность, либо конкатенация буквы из A и элемента из X. Если потребовать, чтобы θ сразу был изоморфизмом, то получится категория, инициальный объект которой — множество конечных слов A^*, а финальный — множество $A^\omega \cup A^*$ конечных и бесконечных слов над A. Ясно, что инициальный объект категории единственным образом отображается в финальный, т.е. A^* естественно вкладывается в $A^\omega \cup A^*$. Мы получили пример естественного отображения индуктивной конструкции в коиндуктивную.

3.1.10. (Пример коиндуктивной конструкции: канторово множество $C = \{0,1\}^{\mathbb{N}}$.) Канторово множество $C = \{0,1\}^{\mathbb{N}}$ бесконечных последовательностей из нулей и единиц также является примером коиндуктивной конструкции, поскольку это частный случай **3.1.8** для алфавита $A = \{0,1\}$. Можно также задать C непосредственно, как финальный объект в категории пар $(C : \mathcal{C}, \theta : C \to C \sqcup C)$, где θ используется для выражения того факта, что любой элемент C имеет либо вид 0α, либо 1α для некоторого $\alpha \in C$.

3.1.11. (Отображение $U : C \to I$.) Коиндуктивное определение отрезка $I = [0,1]$, приведенное в **3.1.7**, по существу определяет его как множество надлежащим образом отождествлённых бесконечных двоичных дробей $(0.x_0x_1x_2\ldots)_2$. В то же время канторово множество $C = \{0,1\}^\omega$ есть множество всех бесконечных последовательностей из нулей и единиц. Поэтому естественно ожидать, что существует каноническое отображение $u : C \to I$, отображающее бесконечную последовательность нулей и единиц в соответствующую двоичную дробь. Такое u можно построить

с помощью универсального свойства I. Для этого изготовим из C «псевдоотрезок» $C' := C \sqcup 1$, взяв $l' := i_1 0^\infty : 1 \to C'$ (см. **3.1.19**, где определён $0^\infty : C$), $r' := i_2 : 1 \to C'$ и определив $\theta' : C' = C \sqcup 1 \to C' \sqcup_{r,l} C' = C \sqcup C \sqcup 1$ как $\theta_C \sqcup \mathrm{id}_1$, где $\theta_C : C \to C \sqcup C$ — структурный морфизм C. Поскольку $(C' = C \sqcup 1, l', r', \theta')$ удовлетворяет условиям из **3.1.7**, существует единственный морфизм $u' : C' \to I$ в финальный объект I. Тогда $u := u' i_1 : C \to I$ — искомый морфизм.

3.1.12. (Пример коиндуктивной конструкции: $\mathbb{Z}_p$.) Ясно, что целые p-адические числа могут быть представлены как бесконечные последовательности над алфавитом из p цифр $\{0, 1, \ldots, p-1\}$. Например, можно отобразить $\sum_{k=0}^{+\infty} c_k p^k$ с $c_k \in \{0, 1, \ldots, p-1\}$ в бесконечную последовательность $(c_0, c_1, \ldots)$, либо воспользоваться представителями Тейхмюллера. Поскольку для вычисления первых нескольких цифр суммы или произведения p-адических чисел достаточно знать первые несколько цифр слагаемых или сомножителей, структура кольца $\mathbb{Z}_p$ оказывается согласованной с его коиндуктивной конструкцией.

3.1.13. (Пределы и копределы как коиндуктивные и индуктивные конструкции.) Отметим, что произвольный предел в категории $\mathcal{C}$ является примером коиндуктивной конструкции, поскольку он определен как финальный объект некоторой категории диаграмм в $\mathcal{C}$, в то время как копределы являются индуктивными конструкциями, поскольку они — инициальные объекты в категориях диаграмм. Например, прямое произведение $A \times B$ есть финальный объект в категории троек $(X : \mathcal{C}, p : X \to A, q : X \to B)$, и потому оно является примером коиндуктивной конструкции с параметрами A и B. Это показывает, что вспомогательные конструкции, используемые при определении категории диаграмм для построения некоторой новой индуктивной или коиндуктивной конструкции, сами могут быть более простыми индуктивными или коиндуктивными конструкциями. При этом индуктивные конструкции могут быть определены с помощью вспомогательных коиндуктивных конструкций (см., например, **3.1.5**, где индуктивная конструкция множества конечных слов $X = A^\omega$ задействует $c : A \times X \to X$ в качестве компонента диаграммы) и наоборот (см., например, коиндуктивное определение отрезка $I = [0, 1]$ в **3.1.7**, где использован пушаут $I \sqcup_{r,l} I$, т.е. индуктивная конструкция).

3.1.14. (Естественные топологии на индуктивных и коиндуктивных конструкциях.) Обычно индуктивные и коиндуктивные конструкции изна-

чально рассматриваются в категории множеств, хотя другие категории тоже могут быть полезны. Так, мы можем повторить любую такую конструкцию, например, индуктивную конструкцию натуральных чисел $N = \mathbb{N}_0$ или коиндуктивную конструкцию отрезка $I = [0, 1]$ в категории (отделимых) топологических пространств. Обычно мы получим то же самое множество, что и при применении этой конструкции в категории множеств, но с некоторой естественной топологией. При этом получающаяся топология на индуктивной конструкции почти всегда будет дискретной. Фактически единственный способ получить недискретное пространство — это применить индуктивную конструкцию к параметру, являющемуся недискретным топологическим пространством, например, можно рассмотреть свободный моноид A^*, порожденный недискретным топологическим пространством A, таким, как отрезок $[0, 1]$ (тогда это будет примером применения индуктивной конструкции к коиндуктивному параметру).

3.1.15. (Полнота естественной равномерной структуры на коиндуктивных конструкциях.) Однако естественная топология на большинстве коиндуктивных конструкций, как правило, недискретна. Например, таким образом получается вещественная топология на $I = [0, 1]$ и p-адическая топология на $\mathbb{Z}_p$. Во многих случаях топология на коиндуктивных конструкциях задается некоторой естественной равномерной структурой (потому что можно применить конструкцию не только в категории топологических пространств, но и в категории отделимых равномерных пространств), и эта равномерная структура обычно полна. Причина этого приблизительно такова: если X — финальный объект в некоторой категории диаграмм в равномерных пространствах, то $\hat{X}$ тоже является диаграммой из этой категории, а значит, $X \to \hat{X}$ обладает ретрактом, т.е. пространство X — ретракт полного отделимого пространства $\hat{X}$, и потому само полно и отделимо. (Чтобы превратить это рассуждение в теорему, надо подробно описать, какие именно вспомогательные конструкции мы допускаем при определении категории диаграмм; эти конструкции должны быть согласованы с функтором пополнения равномерных пространств, а также с забывающим функтором из равномерных пространств в категорию множеств.)

3.1.16. (Естественная топология коиндуктивных конструкций как причина успеха теоретико-множественной топологии в анализе.) Можно предположить, что именно наличие естественной топологии и зачастую пол-

ных равномерных структур является истинной причиной успешности применения (теоретико-множественной) топологии в анализе и близких дисциплинах.

3.1.17. (Конструктивные элементы индуктивных конструкций.) Обычно в индуктивных конструкциях можно выделить *конструктивные элементы*, которые получаются за конечное число шагов из структурных морфизмов индуктивной конструкции (т.е. из компонент соответствующей диаграммы) и, возможно, из элементов параметров индуктивной конструкции (например, элементы индуктивной конструкции $A \sqcup B$ легко строятся из элементов A и элементов B). Это применимо не только в категории множеств, но и в других категориях $\mathcal{C}$, если мы договоримся называть «элементами» $x : X$ объекта $X : \mathcal{C}$ его глобальные сечения, т.е. морфизмы $x : 1_{\mathcal{C}} \to X$ из финального объекта категории $\mathcal{C}$ в X.

Так, если N — объект натуральных чисел, в нем легко строятся конструктивные элементы o, $s(o)$, $s(s(o))$, ..., обычно обозначаемые как 0, 1, 2, ... В общем случае конструктивные элементы обычно могут быть записаны как конечные формулы, в которых могут участвовать элементы параметров индуктивной конструкции.

3.1.18. (Все элементы индуктивных конструкций обычно конструктивны.) Обычно все элементы индуктивных конструкций оказываются конструктивны, просто потому, что подмножество (или подтип, подобъект...), составленное из конструктивных элементов, уже обладает универсальным свойством индуктивной конструкции. Иначе говоря, индуктивные конструкции минимальны, в них нет лишних элементов, и есть ровно то, что обязано быть — то есть конструктивные элементы.

3.1.19. (Конструктивные элементы коиндуктивных конструкций.) Можно аналогичным образом определить конструктивные элементы коиндуктивных конструкций. Однако при их определении необходимо разрешить (конечное число раз) использовать не только структурные морфизмы коиндуктивной конструкции и элементы ее параметров, но и универсальное свойство коиндуктивной конструкции, иначе может оказаться, что мы не можем построить ни одного элемента.

Проиллюстрируем это на примере прямого произведения $X = A \times B$. Это финальный объект в категории диаграмм $(X, p : X \to A, q : X \to B)$. Поскольку нет структурных морфизмов со значениями в X, непонятно, откуда взять хотя бы один элемент $X = A \times B$. Однако если $a : A$ и $b : B$ (т.е. $a : 1 \to A$ и $b : 1 \to B$) — произвольные элементы A и B, то $(1, a : 1 \to$

$A, b : 1 \to B$) — объект рассматриваемой категории диаграмм, и потому из него есть морфизм (a, b) в финальный объект $A \times B$, т.е. существует единственный элемент $(a, b) : 1 \to A \times B$, такой, что $p(a, b) = a$ и $q(a, b) = b$. Как обычно, мы разрешаем использовать такие элементы в формулах, если они определяются с помощью свойства, которому удовлетворяет единственный объект (см. обсуждение ι-символа Гильберта в **3.3.1**).

Более сложный пример — это бесконечные слова A^ω из **3.1.8**. В этом случае у нас есть только структурный морфизм деконкатенации (разложения) $\theta : A^\omega \to A \times A^\omega$, и мы можем доказать, что он является изоморфизмом. Поэтому мы в принципе можем строить выражения $\theta^{-1}(x, \alpha) : A^\omega$ с помощью конкатенации θ^{-1}, в которых $x : A$ и $\alpha : A^\omega$. Одна проблема: у нас нет ни одной константы со значениями в A^ω, поэтому нам не с чего начать построение бесконечных слов. Для решения этой проблемы выберем произвольный элемент $a : A$ (что означает $a \in A$ в категории множеств либо $a : 1 \to A$ в произвольной категории $\mathcal{C}$) и заметим, что $(a, *)$ есть элемент прямого произведения $A \times 1$, а значит, $\big(1, (a, *) : 1 \to A \times 1\big)$ есть объект из категории диаграмм, финальным объектом которой является A^ω. Универсальное свойство A^ω теперь позволяет нам определить морфизм $a^\infty : 1 \to A^\omega$, т.е. элемент $a^\infty : A^\omega$, такой, что $\theta(a^\infty) = (a, a^\infty)$, что на самом деле означает, что a^∞ — последовательность $aaa\ldots$ из бесконечного количества экземпляров a. После того, как мы построили $a^\infty : A^\omega$ для любого $a : A$, мы легко можем построить, например, бесконечные слова $abc^\infty = abcccc\ldots = \theta^{-1}(a, \theta^{-1}(b, c^\infty)) : A^\omega$ для любых a, b, $c \in A$, т.е. в действительности A^ω содержит много конструктивных элементов.

Отметим, что элементы указанного вида не исчерпывают всех конструктивных элементов A^ω: например, можно доказать с помощью универсальных свойств, что $(A \times A)^\omega \cong A^\omega$, и использовать этот изоморфизм для построения бесконечных слов $(ab)^\infty = ababab\ldots$, характеризуемых взаимно рекурсивными свойствами $\theta((ab)^\infty) = (a, (ba)^\infty)$ и $\theta((ba)^\infty) = (b, (ab)^\infty)$. В действительности, если $x : N \to A$ — произвольная последовательность элементов A (т.е. морфизм в $\mathcal{C}$ из объекта натуральных чисел N в A), то можно построить элемент $\boldsymbol{x} = u(x) : A^\omega$, такой, что $\theta\big(u(x)\big) = \big(x(0), x \circ s\big)$; если $\mathcal{C} = \mathit{Sets}$, это означает, что любой последовательности $(x_n)_{n\in\mathbb{N}_0}$ можно сопоставить бесконечное слово $\boldsymbol{x} = x_0x_1x_2\ldots$. Для доказательства этого факта надо построить диаграмму $(N, \theta_x : N \to A \times N)$, где $\theta_x(n) = (x(n), n + 1)$, и применить к ней универсальное свойство A^ω. Если категория $\mathcal{C}$ декартово замкнута,

мы получим таким образом морфизм $u : A^N = \mathbf{Hom}(N, A) \to A^\omega$; если $\mathcal{C}$ топос, то этот морфизм будет изоморфизмом.

С другой стороны, в каких-то случаях в коиндуктивных конструкциях X есть «константы», т.е. готовые морфизмы из 1 или из одного из параметров конструкции в X. Например, в случае отрезка $I = [0, 1]$ есть константы $0 = l$ и $1 = r$, а также морфизм $\theta : I \to I \sqcup_{r,l} I$, про который можно доказать, что он изоморфизм. Поэтому мы можем применять $\theta^{-1} \circ i_1 : I \to I \sqcup_{r,l} I \xrightarrow{\sim} I$ и $\theta^{-1} \circ i_2 : I \to I$ к этим константам для построения конструктивных элементов I. Поскольку эти два отображения $I \to I$ соответствуют $x \mapsto x/2$ и $x \mapsto (x + 1)/2$, получающиеся таким образом конструктивные элементы $I = [0, 1]$ — это двоично-рациональные числа, причем для их построения не используется универсальное свойство I (кроме как для доказательства того, что θ — изоморфизм). С другой стороны, если явно использовать универсальное свойство I, можно построить другие конструктивные элементы I, например, элементы $1/3$ и $2/3$, характеризуемые $\theta(1/3) = i_1(2/3)$ и $\theta(2/3) = i_2(1/3)$. Более общо, любая бесконечная двоичная дробь $0.x_0x_1\ldots$ (т.е. любая функция $x : N \to \{0, 1\} = 1 \sqcup 1$) задает некоторый элемент I (для доказательства надо взять псевдоотрезок $X = 1 \sqcup N \sqcup 1$, где $n : N$ неформально соответствует бесконечной дроби $0.x_nx_{n+1}\ldots$, и построить $\theta_x : X \to X \sqcup_{r,l} X$ с помощью функции x по формуле $\theta_x(n) = i_{1+x_n}(n + 1)$, затем применить универсальное свойство I). Если функция x конструктивна, можно считать такие бесконечные двоичные дроби конструктивными элементами I. Например, $1/\sqrt{2}$ — конструктивный элемент I, соответствующий функции $x(n) = \max\{y \in N : y^2 \leq 2^{2n+1}\} \bmod 2$.

3.1.20. (Альтернативная конструкция отрезка I.) Конструкция отрезка $I = [0, 1]$ через бесконечные двоичные дроби **3.1.7** является самой простой, но не всегда самой удобной для приложений. Например, не из всякой конструктивной фундаментальной последовательности рациональных чисел, заключённых между нулём и единицей, можно автоматически построить элемент I. Более того, не удаётся даже определить отображение $s : I \times I \to I$, соответствующее полусумме $s(x, y) = (x + y)/2$, из-за того, что при сложении бесконечных двоичных дробей очередная цифра суммы может зависеть от бесконечного количества цифр слагаемых.

Можно предложить другие коиндуктивные конструкции отрезка, более сложные, но лишённые этих недостатков. Например, можно записывать числа $x \in [0, 1]$ с помощью избыточной двоичной системы: $x =$

$\sum_{n=0}^{\infty} x_n 2^{-n-2}$, где $x_n \in \{0,1,2\}$, тогда первые n цифр суммы могут быть вычислены по первой $n+2$ цифрам слагаемых. Иначе говоря, альтернативный отрезок I' обладает двумя различными константами $0, 1 : 1_{\mathcal{C}} \to I'$ и тремя отображениями l, m, $r : I' \to I'$, соответствующими $x \mapsto x/2$, $x \mapsto x/2 + 1/4$ и $x \mapsto (x+1)/2$. При этом должны быть выполнены некоторые аксиомы, такие, как $ml = lr$, $mr = rl$, $l0 = 0$, $r1 = 1$, $l1 = r0$, и следующая коммутативная диаграмма должна быть копределом:

$$\begin{array}{ccccc} * & \xrightarrow{0} & I' & \xrightarrow{l} & I' \\ \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle r} & & \\ I' & \xrightarrow{l} & I' & & \downarrow{\scriptstyle r} \\ \downarrow{\scriptstyle r} & & & \searrow{\scriptstyle m} & \\ I' & & \xrightarrow{\quad l \quad} & & I' \end{array} \tag{3.1.20.1}$$

В обычной теории типов можно обойтись без левого верхнего угла, равно как и без констант 0 и 1 (они нужны только для аксиомы $0 \neq 1$), но всё это необходимо для правильного определения I' в гомотопической теории типов. С другой стороны, для обычного отрезка I из **3.1.7** мы можем построить такую коммутативную диаграмму (без диагональной стрелки m), причём и маленький квадрат в верхнем левом углу, и внешний контур диаграммы будут кодекартовыми квадратами. Отсюда следует существование стрелки m для I, а значит, и канонического морфизма $\varphi : I \to I'$ согласно универсальному свойству I'. Этот морфизм, по всей видимости, в общем случае не будет изоморфизмом (хотя, конечно же, будет им в категории множеств), потому что мы можем определить полусумму $s : I' \times I' \to I'$ на I', но не на I.

Однако при таком подходе сложно скомбинировать l, m, r в один морфизм из I' в некоторый конечный копредел и при этом описать все необходимые отождествления, а без этого сложно применять универсальное свойство I'. Возможно, проще сначала построить $\mathbf{3}^{\omega} = \{0,1,2\}^{\omega}$, а затем построить I' как его факторобъект с помощью подходящей коиндуктивной конструкции.

3.1.21. (Альтернативный отрезок I' как $[-1,1]$, построение $\mathbb{R}$ из I'.) Альтернативный отрезок I' зачастую удобней отождествлять с вещественными числами $[-1,1]$, а не $[0,1]$. В этом случае отображения l, m, $r : I' \to I'$ соответствуют $l(x) = (x-1)/2$, $m(x) = x/2$, $r(x) = (x+1)/2$, а константы 0

и 1 становятся константами -1 и 1, с теми же характеристическими свойствами $l(-1) = -1$, $r(1) = 1$. Соответствие между числами $x \in [-1, 1]$ и их избыточными двоичными записями лучше теперь записывать в виде $x = \sum_{n=0}^{\infty} x_n 2^{-n-1}$, где $x_n \in \{-1, 0, 1\}$; иногда удобней писать $\bar{1}$ вместо -1, например, $1/\pi = (0.1\bar{1}1\bar{1}0010\bar{1}0000\bar{1}\ldots)_2$.

3.1.22. (Построение $\mathbb{R}$ и $\mathbb{Q}_p$ из I' и $\mathbb{Z}_p$.) При таком подходе естественно строить $\mathbb{R}$ из $I' = [-1, 1]$ с помощью вспомогательной индуктивной конструкции как индуктивный предел последовательности морфизмов $I' \xrightarrow{m} I' \xrightarrow{m} I' \xrightarrow{m} \ldots$; тем самым $\mathbb{R}$ — это нечто вроде локализации I' относительно m, т.е. умножения на $1/2$. Аналогично, $\mathbb{Q}_p$ может быть построено из $\mathbb{Z}_p$ как индуктивный предел $\mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \xrightarrow{p} \ldots$, где $p : \mathbb{Z}_p \to \mathbb{Z}_p$ обозначает умножение на p (оно может быть легко задано, например, с помощью сдвига последовательности цифр, задающих элемент $\alpha \in \mathbb{Z}_p$, на одну позицию). Отметим, что гипотетически можно строить $\mathbb{R}$ и с помощью стандартного отрезка I из **3.1.7**, но в этом случае не удается даже задать сложение на $\mathbb{R}$, в то время как альтернативный отрезок I' из **3.1.21** позволяет определить сложение и умножение вещественных чисел.

Тем самым $\mathbb{R}$ и $\mathbb{Q}_p$, в отличие от $[-1, 1]$ и $\mathbb{Z}_p$, не являются чисто коиндуктивными конструкциями. Они являются индуктивно-коиндуктивными конструкциями, т.е. они получаются применением индуктивной конструкции к коиндуктивному аргументу.

3.1.23. (Умножение $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ и $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$.) Заметим, что отображение умножения вещественных чисел $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x, y) \mapsto xy$, конструктивно, однако является непрерывным, но не равномерно непрерывным, что на первый взгляд противоречит тому, что было сказано выше в **3.1.15** про каноничность равномерных структур на коиндуктивных конструкциях. Аналогичная ситуация и с p-адическим умножением $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$. В действительности здесь нет противоречия, поскольку $\mathbb{Q}_p$ и $\mathbb{R}$ не чисто коиндуктивные конструкции, а индуктивно-коиндуктивные, см. **3.1.22**.

Можно также отметить, что чисто коиндуктивные конструкции, такие, как I и $\mathbb{Z}_p$ (использующие только конечные множества как аргументы), зачастую оказываются не только полны, но и компактны, что отчасти объясняет, почему заданные на них непрерывные отображения оказываются равномерно непрерывны.

3.1.24. (Не все элементы коиндуктивных конструкций конструктивны,

но конструктивные элементы обычно плотны.) Отметим, что в отличие от элементов индуктивных конструкций, не все элементы коиндуктивных конструкций конструктивны. Однако конструктивные элементы обычно плотны в естественной топологии, которую мы определили в **3.1.14**. Поскольку обычно множество конструктивных элементов счетно (потому что конструктивные элементы могут быть заданы конечными формулами и выражениями), мы видим, что *коиндуктивные конструкции обычно являются полными равномерными пространствами, а конструктивные элементы часто образуют счетное всюду плотное множество*. Эта плотность тоже может быть строго доказана для некоторых классов диаграмм, но мы не будем сейчас этим заниматься.

3.1.25. (Коиндуктивные конструкции часто являются польскими пространствами и обладают мощностью континуум.) Предыдущие рассуждения показывают, что зачастую коиндуктивные конструкции X допускают полную равномерную структуру, относительно которой есть счетное всюду плотное множество. Если доказать, что эта равномерная структура порождается счетным семейством окружений — то есть что X метризуемо — то тем самым X окажется польским пространством. Примем без доказательства, что это действительно так во многих случаях (см. также **3.1.26** ниже). Поскольку все несчетные польские пространства обладают мощностью континуум, это объясняет, почему почти все интересные множества в анализе и в математике вообще либо счетны (индуктивные конструкции), либо обладают мощностью континуум (коиндуктивные конструкции). В этом смысле континуум-гипотеза верна.

3.1.26. (Метризуемость коиндуктивных конструкций: конструктивные окружения равномерной структуры.) Неформально поясним, почему естественная равномерная структура на коиндуктивных конструкциях часто оказывается порожденной счетным семейством окружений, т.е. метризуемой. Пусть X — коиндуктивная конструкция с параметрами A_1, ..., A_n. Будем предполагать, что естественные равномерные структуры на параметрах A_i дискретны (это обычно будет так, если A_i сами заданы с помощью индуктивных конструкций) или хотя бы метризуемы (например, если A_i заданы с помощью более простых коиндуктивных конструкций, они метризуемы «по предположению индукции»). Таким образом, можно считать, что на каждом A_i фиксировано счетное фундаментальное семейство окружений. Будем строить всевозможные конструктивные отображения из X в A_i (на самом деле не только в параметры A_i, но и

в некоторые другие вспомогательные конструкции, например, конечные множества), т.е. отображения, которые могут быть построены с помощью конечного числа применений структурных морфизмов X, универсального свойства X и каких-то стандартных конструкций. Поскольку конструктивные отображения $p : X \to A_i$ обычно задаются конечными формулами, их будет не более чем счетное множество. С другой стороны, естественная равномерная структура на X обычно будет самой слабой равномерной структурой, в которой все p равномерно непрерывны. Это означает, что равномерная структура X порождается прообразами относительно всевозможных $p : X \to A_i$ окружений из выбранных фундаментальных счетных семейств окружений на A_i. Потому она тоже обладает счетным порождающим семейством, т.е. метризуема.

Можно сказать, что метризуемость равномерной структуры X является следствием счётности множества «конструктивных» окружений, а оно счетно, поскольку конструктивные окружения параметризуются конечными формулами, аналогично множеству конструктивных элементов X. В этом смысле метризуемость равномерной структуры является двойственным свойством к наличию счётного всюду плотного подмножества (конструктивных элементов).

3.1.27. (Чистые индуктивные и коиндуктивные конструкции тривиальны.) Мы видели в **3.1.22**, что $\mathbb{R}$ и $\mathbb{Q}_p$ не являются чисто коиндуктивными конструкциями, а являются индуктивно-коиндуктивными, т.е. являются результатом применения индуктивной конструкции к коиндуктивному аргументу. Однако отрезок $I' = [-1, 1]$ и $\mathbb{Z}_p$ в действительности также не являются чисто коиндуктивными конструкциями. Например, в построении $\mathbb{Z}_p$ как $\{0, 1, \ldots, p-1\}^\omega$ коиндуктивная конструкция $A \rightsquigarrow A^\omega$ применяется к конечному p-элементному множеству, которое является индуктивной конструкцией, а именно, копроизведением p экземпляров финального объекта (или одноточечного множества). Точно так же канторово множество $C = \{0, 1\}^\omega$ использует либо двухэлементное множество $\{0, 1\} = 1 \sqcup 1$ в качестве параметра, либо определяется как финальный объект в категории пар $(C, \theta : C \to C \sqcup C)$, и тогда копроизведение, т.е. индуктивная конструкция, задействуется при построении категории диаграмм.

Рассуждая таким образом, несложно прийти к выводу, что все чисто коиндуктивные конструкции (т.е. коиндуктивные конструкции, которые используют только ранее определенные чисто коиндуктивные конструк-

ции для построения категории диаграмм или в качестве параметров) оказываются изоморфны финальному объекту 1 (т.е. одноточечному множеству, если $\mathcal{C} = Sets$). Аналогично, единственная чисто индуктивная конструкция — это инициальный объект $\varnothing$ (пустое множество). Применяя индуктивные конструкции (копроизведение) к чисто коиндуктивному параметру (финальному объекту), мы получаем конечные, а затем и бесконечные множества, такие, как множество натуральных чисел. Применяя к конечным множествам коиндуктивные конструкции, при определении которых мы также разрешаем использовать конечные копределы, мы получаем коиндуктивные конструкции вроде $\mathbb{Z}_p$ или I'. Мы можем, однако, строить коиндуктивные конструкции с бесконечными индуктивными параметрами, такие, как N^ω (бесконечные последовательности натуральных чисел).

3.1.28. (Сложность математических объектов как количество изменений кванторов. Многомерные локальные поля.) Напомним, что в математической логике применяется следующая грубая классификация формул по сложности: более сложной считается та формула, в которой больше перемен кванторов (с $\forall$ на $\exists$ и наоборот) во вложенных цепочках кванторов. При этом все свободные переменные можно считать связанными квантором всеобщности. Например, в условии коммутативности $(\forall x)(\forall y)(x + y = y + x)$ нет перемен кванторов, а в определении непрерывности $(\forall x)(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x')(|x - x'| < \delta \Rightarrow |f(x) - f(x')| < \varepsilon)$ есть целых две перемены кванторов. Поэтому непрерывность функции — более сложное свойство, чем коммутативность операции.

Мы можем аналогичным образом классифицировать математические конструкции по количеству переходов от коиндуктивным конструкций к вложенным индуктивным и наоборот (это тем более естественно, если учесть, что $(\forall x : X)(P(x))$ с точки зрения теории типов является зависимым произведением $\prod_{(x:X)} P(x)$, т.е. коиндуктивной конструкцией, а $\exists x$ — индуктивной). В качестве базы можно использовать ничто (тогда первым шагом любого построения всегда будет построение финального объекта, т.е. коиндуктивная конструкция, к которой применяется копроизведение, т.е. индуктивная конструкция), либо можно начать сразу с конечных множеств. С такой точки зрения натуральные числа $\mathbb{N}_0$, целые p-адические числа $\mathbb{Z}_p$ и отрезок $I' = [-1, 1]$ обладают одинаковой «сложностью», а $\mathbb{R}$ и $\mathbb{Q}_p$ — более сложны, поскольку они получаются из конечных множеств и конструкций с помощью индуктивно-коиндуктивной

конструкции. Это проявляется и в том, что $\mathbb{Z}_p$ и I' компактны, в то время как $\mathbb{R}$ и $\mathbb{Q}_p$ — всего лишь локально компактны. Если считать, что индуктивные конструкции, применённые к конечным множествам, дают счётные множества с дискретной топологией, а коиндуктивные — польские компакты (т.е. отделимые компактные пространства со счётной базой топологии), то индуктивно-коиндуктивные дадут в лучшем случае локально компактные, а то и компактно-порождённые пространства. Следующая итерация — коиндуктивно-индуктивно-коиндуктивные конструкции, применённые к конечным множествам — по всей видимости задаёт математические объекты, для описания которых уже не хватает топологии. Многомерные локальные поля при правильном подходе как раз являются примерами подобных конструкций. Возможно, именно поэтому с ними не удаётся управляться привычными (топологоалгебраическими) средствами.

3.1.29. (Элементы коиндуктивных конструкций могут быть представлены фундаментальными последовательностями конструктивных элементов.) Отметим, что, поскольку коиндуктивная конструкция X зачастую оказывается полна, а множество конструктивных элементов в ней счётно и всюду плотно, произвольный элемент $x \in X$ может быть записан как предел некоторой сходящейся, или, что равносильно, фундаментальной последовательности (x_n) конструктивных элементов. Например, любое вещественное или p-адическое число есть предел некоторой последовательности рациональных чисел.

3.1.30. (Не все элементы коиндуктивных конструкций конструктивны, но сами коиндуктивные конструкции конструктивны.) Несмотря на то, что не все элементы коиндуктивных конструкций конструктивны, сами коиндуктивные конструкции конструктивны, по крайней мере, если категория диаграмм, используемая для их построения, допускает описание с помощью конечного числа формул и вспомогательных конструкций, все из которых конструктивны. Это так, поскольку коиндуктивные конструкции являются финальными объектами в этих категориях диаграмм, т.е. однозначно определены своим универсальным свойством. Таким образом, например, $I = [0, 1]$ и $\mathbb{R}$ конструктивны, несмотря на то, что конструктивных вещественных чисел очень мало (их счетное множество).

3.1.31. (Промежуточный итог: коиндуктивные конструкции не менее естественны, чем индуктивные, и имеют право на существование, осо-

бенно в теории чисел.) Подведем промежуточный итог. Мы видим, что индуктивные конструкции обычно счетны, на них нет естественной топологии, помимо дискретной, и все их элементы обычно конструктивны, т.е. задаются конечными формулами. Поэтому индуктивные конструкции очень часто возникают в алгебре и логике. С другой стороны, коиндуктивные конструкции обычно обладают мощностью континуум, и на них есть естественная топология и равномерная структура, в которой они полны и являются польскими пространствами. Конструктивных элементов в них мало, но они зачастую образуют счетное всюду плотное множество. Коиндуктивные конструкции естественным образом возникают в анализе, и они не менее конструктивны и естественны, чем индуктивные конструкции. Более того, в теории чисел уже используются не только индуктивные, но и коиндуктивные конструкции, например, $\mathbb{Z}_p$. Поэтому предположение, что абсолютная база, необходимая для построения абсолютной геометрии, в которой бы числовой случай стал бы аналогичен функциональному, может задействовать для своего построения как индуктивные, так и коиндуктивные конструкции, ничему не противоречит и даже ожидаемо.

3.2 Коиндуктивные конструкции в теории вероятностей

Мы видели, что коиндуктивные конструкции не менее естественны, чем индуктивные, и что они зачастую естественным образом возникают в анализе и близких дисциплинах. Как следствие, они оказываются связаны и с теорией вероятностей, например, в рамках колмогоровской аксиоматизации теории вероятностей, увязывающей вероятность и теорию меры. Можем ли мы более явно проследить возникновение коиндуктивных конструкций в теории вероятностей?

3.2.1. (Элементы канторова множества $C = \{0,1\}^\omega$ как источник случайных последовательностей нулей и единиц.) Первое наше наблюдение будет вот каким. Заметим, что канторово множество $C = \{0,1\}^\omega$, описанное как коиндуктивная конструкция в **3.1.10**, обладает лишь одним структурным морфизмом $\theta : C \to C \sqcup C \cong \{0,1\} \times C$. Потому, если нам дан элемент $\alpha : C$, единственное, что мы с ним можем сделать с вычислительной или конструктивной точки зрения — это применить θ и получить $\theta(\alpha) = (x_0, \alpha')$, где $x_0 \in \{0,1\}$ и $\alpha' : C$. Иначе говоря, мы полу-

чаем одну двоичную цифру и новый элемент C, с которым мы, в свою очередь, можем разве что снова повторить эту операцию. Тем самым элементы $\alpha : C$ можно рассматривать как генераторы последовательностей из нулей и единиц. После получения очередной двоичной цифры мы заодно получаем и новое состояние генератора. При этом, если элемент $\alpha : C$ «произволен» или «случаен» (относительно естественной вероятностной меры на $\{0,1\}^{\mathbb{N}}$), то получающаяся последовательность нулей и единиц будет случайной, т.е. C — это генератор независимых случайных двоичных цифр, или «источник случайности».

3.2.2. (Элемент $\alpha : C$ как источник более сложных случайных объектов.) Мы можем извлекать из этого генератора сразу несколько цифр подряд и использовать их вместе для генерации более сложных объектов. Например, взяв три двоичные цифры, т.е. применив θ три раза, мы можем выбрать «случайный» элемент из любого (не более чем) восьмиэлементного множества. Более того, мы можем использовать префикс-код для кодирования всех (конструктивных) элементов какой-нибудь индуктивной конструкции A, и читать по цифре из $\alpha : C$ до тех пор, пока не увидим полный код какого-то элемента A. Например, мы можем кодировать натуральное число $n : N$ с помощью слова 1^n0; тогда для получения случайного натурального числа мы будем генерировать случайные двоичные цифры до тех пор, пока не получим ноль; количество единиц, сгенерированных до первого нуля, и есть искомое случайное натуральное число.

3.2.3. (Распределение вероятностей на элементах индуктивных конструкций.) В предыдущем примере мы не просто получаем случайные элементы индуктивных конструкций, например, случайные натуральные числа, но получаем их с некоторыми фиксированными вероятностями. Например, мы получаем число $n \geq 0$ с вероятностью 2^{-n-1}. В общем случае мы строим некоторое конструктивное отображение $\gamma : C \to A \times C$, где A — заданная индуктивная конструкция. Тогда на A возникает естественная мера — образ стандартной вероятностной меры ν_C на C (будем называть её «мерой Хаара на C») относительно отображения $p = \mathrm{pr}_1 \circ \gamma : C \to A$. Поскольку индуктивные конструкции (в категории множеств) обычно счётны и дискретны, вероятностные меры на A задаются просто перечислением вероятностей всех элементов: $p_a := P(\xi = a)$ для $a \in A$ с $p_a \geq 0$, $\sum_{a \geq 0} p_a = 1$, т.е. они параметризуются (пополненным бесконечномерным) симплексом $\hat{\Delta}^{(A)}$.

Отметим, что для задания вероятностных распределений на A нам на самом деле не обязательно изначально располагать теорией меры: мы можем вместо этого изучать отображения $C \to A$, конструктивные или нет. Иначе говоря, понятие процесса порождения случайного элемента типа A при желании может быть использовано вместо понятия случайной величины, т.е. измеримой функции, для обоснования некоторых фрагментов теории вероятностей. Тем самым формально исключается необходимость использования теории меры. При этом получающаяся теория может быть более общей, например, она может быть применима не только в категории множеств.

3.2.4. (Случайные элементы коиндуктивных конструкций.) Помимо случайных элементов индуктивных конструкций, нам могут быть полезны случайные элементы коиндуктивных конструкций, например, случайные элементы отрезка $I = [0, 1]$. Если мы хотим получить равномерно распределенную случайную величину на $[0, 1]$, достаточно взять отображение $U : C \to I$, построенное в **3.1.11**, которое переводит бесконечную последовательность нулей и единиц в вещественное число с соответствующей двоичной записью. Это U конструктивно, и переводит меру Хаара ν_C на C в меру Лебега на $[0, 1]$. Далее, если $F : \mathbb{R} \to [0, 1]$ — любая непрерывная функция распределения, мы можем построить случайную величину с таким распределением как $F^{-1} \circ U$, и эта конструкция конструктивна, если функция F конструктивна. Например, мы можем определить случайную стандартную гауссовскую величину.

3.2.5. (Произвольные вероятностные распределения на индуктивных конструкциях.) Заметим, что умение генерировать равномерно распределенные случайные величины с помощью $U : C \to [0, 1]$ сразу позволяет генерировать случайные величины со значениями в фиксированном счётном множестве A, например, в некоторой индуктивной конструкции, если задано произвольное (желательно конструктивное) распределение вероятностей $p_a \geq 0$ на A, $\sum_{a \in A} p_a = 1$. Например, если $A = N = \mathbb{N}_0$, мы можем вычислить кумулятивные суммы $P_n := \sum_{m=0}^{n-1} p_m$ и затем отобразить $\varphi : [0, 1] \to N$ с помощью $\varphi : x \mapsto \max\{n \in N : P_n \leq x\}$. Тогда образ меры Лебега на $[0, 1]$ относительно φ — это требуемая вероятностная мера на N, так что $\varphi \circ U$ может использоваться для задания случайной величины на N с заданным распределением. Отметим, что отображение φ не совсем определено с конструктивной точки зрения, даже если исходное вероятностное распределение конструктивно; одна-

ко оно определено всюду, кроме некоторого множества меры нуль, что достаточно для наших целей. (Это довольно ожидаемо, потому что все конструктивные отображения непрерывны, а φ не непрерывно; в то же время конструктивные отображения, определённые почти всюду, всего лишь измеримы.)

3.2.6. (Расщепление генератора: «диагональ» $\Delta : C \to C \times C$.) Когда мы генерировали, например, случайные натуральные числа, мы строили отображение $\gamma : C \to N \times C$, которое дает из «генератора случайных чисел» или «источника случайности» $\alpha : C$ не только случайное число n, но и новый генератор $\alpha' : C$, который мы затем можем использовать для генерации последующих случайных элементов, независимых от уже построенного. Однако генерация одного числа $x : [0,1]$ расходует сразу весь запас случайности, поскольку у нас есть отображение $U : C \to I = [0,1]$, а не $C \to I \times C$. Было бы полезно иметь отображение $U' : C \to I \times C$, которое позволяло бы и дальше генерировать случайные объекты, независимые от уже построенного числа на отрезке $[0,1]$. Тогда мы могли бы, например, сгенерировать последовательность независимых одинаково распределенных случайных величин.

В действительности мы всегда можем это сделать, поскольку существует конструктивное диагональное отображение $\Delta : C \xrightarrow{\sim} C \times C$, которое отображает последовательность двоичных цифр $\alpha = x_0x_1x_2x_3\ldots$ в пару независимых последовательностей $\alpha^{\mathrm{ev}} = x_0x_2x_4\ldots$ и $\alpha^{\mathrm{od}} = x_1x_3x_5\ldots$. Поскольку $\Delta_*(\nu_C) = \nu_C \otimes \nu_C$, мы можем использовать α^{ev} и α^{od}, полученные из $\alpha : C$ с помощью $\Delta(\alpha) = (\alpha^{\mathrm{ev}}, \alpha^{\mathrm{od}})$, для построения независимых случайных объектов. Например, мы можем полностью израсходовать одно из них на построение случайного числа $[0,1]$. Иначе говоря, мы можем из $U : C \to I = [0,1]$ построить $U' : C \to I \times C$ как $U' := (U \times \mathrm{id}_C) \circ \Delta$.

Мы видим, что ключевым является существование конструктивного «коумножения» $\Delta : C \to C \times C$, такого, что $\Delta_*\nu_C = \nu_C \otimes \nu_C$. Это коумножение, однако, не является коассоциативным или кокоммутативным.

3.2.7. (При конструктивном подходе C играет роль вероятностного пространства Ω.) Тем самым выше изложен некоторый конструктивный подход к теории вероятностей, при котором мы описываем, как можно сгенерировать все нужные нам случайные объекты, исходя из одного элемента $\alpha : C$, который можно считать генератором случайных двоичных цифр. Роль A-значной случайной величины ξ при этом выполняется (желательно конструктивными) отображениями $\xi : C \to A$. Поскольку конструк-

тивные отображения, определённые почти всюду (т.е. с вероятностью один), измеримы, мы видим, что это примерно соответствует колмогоровской аксиоматизации, если в качестве вероятностного пространства Ω взять канторово множество C с его стандартной мерой ν_C. Это тем более естественно, если учесть, что (C, ν_C) (вместе с пополнением борелевской σ-алгебры множеств) — это одна из эквивалентных реализаций стандартного вероятностного пространства, см. [AB1],**2.1.10**.

3.2.8. (Прямая коиндуктивная конструкция стандартного вероятностного пространства Ω.) Мы видели в **3.2.6**, что ключевым для использования канторова множества C в качестве (конструктивного) стандартного вероятностного пространства Ω является наличие «диагонали» $\Delta : \Omega \to \Omega \times \Omega$, которая к тому же оказывается изоморфизмом. Это подсказывает, что мы могли бы попытаться напрямую определить Ω с помощью коиндуктивной конструкции, одним из элементов которой является $(\Delta : \Omega \to \Omega \times \Omega)$. К сожалению, если мы просто возьмём финальный объект в категории диаграмм $(\Omega : \mathcal{C}, \Delta : \Omega \to \Omega \times \Omega)$ в какой-нибудь декартовой категории $\mathcal{C}$, то этим финальным объектом окажется $1_{\mathcal{C}}$, т.е. одноточечное множество для $\mathcal{C} = \mathit{Sets}$. Это является примером феномена, отмеченного в **3.1.27**: финальный объект в категории $(\Omega : \mathcal{C}, \Delta : \Omega \to \Omega \times \Omega)$ — это чисто коиндуктивная конструкция, поскольку в качестве вспомогательных элементов используется только прямое произведение, тоже коиндуктивная конструкция, так что Ω оказывается чисто коиндуктивной конструкцией, и потому тривиально.

3.2.9. (Уточнение коиндуктивной конструкции Ω.) Надо добавить дополнительные требования. Например, можно потребовать, чтобы существовала возможность генерировать случайные двоичные цифры, т.е. постулировать существование $c : \Omega \to \{0, 1\}$. Финальный объект в категории диаграмм $(\Omega : \mathcal{C}, \Delta : \Omega \to \Omega \times \Omega, c : \Omega \to \{0, 1\})$, или, что равносильно, в категории диаграмм $(\Omega : \mathcal{C}, d = (c, \Delta) : \Omega \to \{0, 1\} \times \Omega \times \Omega)$ действительно изоморфен канторовому множеству C. В самом деле, из второго описания видно, что Ω — это множество (или тип) бесконечных двоичных деревьев, каждой вершина которых помечена нулём или единицей, $c : \Omega \to \{0, 1\}$ возвращает метку корня, а $\Delta : \Omega \to \Omega \times \Omega$ отображает дерево в пару, состоящую из его левого поддерева и правого поддерева. Эквивалентное описание — Ω есть множество отображений $x : \{0, 1\}^* \to \{0, 1\}$ из конечных двоичных слов в $\{0, 1\}$, $c(x) = x(\varnothing)$ и $\Delta(x) = \big(\alpha \mapsto x(0\alpha), \alpha \mapsto x(1\alpha)\big)$. Если сопоставить двоичному слову

$\alpha \in \{0,1\}^*$ (ненулевое) натуральное число $(1\alpha)_2$, получаем эквивалентное описание: Ω есть $\{0,1\}^{\mathbb{N}}$, c отображает $x = (x_n)_{n\in\mathbb{N}}$ в x_1, а Δ переводит $x_1x_2x_3\ldots$ в пару $(x_2x_4x_6\ldots, x_3x_5x_7\ldots)$. Это отображение очень похоже на $\Delta : C \to C \times C$ из **3.2.6**, но не вполне совпадает с ним, поскольку x_1 не используется в правой части. В итоге наше $\Delta : \Omega \to \Omega \times \Omega$ не является изоморфизмом; изоморфизмом оказывается $d = (c, \Delta) : \Omega \xrightarrow{\sim} \{0,1\} \times \Omega \times \Omega$, что несколько странно, поскольку получается, что при расщеплении генератора случайных чисел почему-то надо заодно сгенерировать одну независимую случайную двоичную цифру.

Если мы хотим избавиться от этого недостатка, надо потребовать, чтобы случайная двоичная цифра, сгенерированная с помощью $c : \Omega \to \{0,1\}$, совпадала со случайной двоичной цифрой, сгенерированной, например, левым генератором после расщепления, т.е. наложить дополнительное условие $c = c \circ \mathrm{pr}_1 \circ \Delta$. В этом случае Ω, $\Delta : \Omega \to \Omega \times \Omega$ и $c : \Omega \to \{0,1\}$ в точности будут совпадать с соответствующими отображениями, ранее построенными для канторова множества, и Δ будет изоморфизмом.

3.2.10. (Итог: теория вероятностей со стандартным вероятностным пространством Ω порождается простой коиндуктивной конструкцией.) Мы видим, что теория вероятностей — или некоторый её конструктивный аналог — естественным образом порождается простой коиндуктивной конструкцией. А именно, мы требуем, чтобы тип «генератора случайных объектов» или «источника случайности» Ω обладал расщеплением $\Delta : \Omega \to \Omega \times \Omega$ и возможностью генерировать случайные двоичные цифры $c : \Omega \to \{0,1\}$, возможно, с дополнительным условием $c = c \circ \mathrm{pr}_1 \circ \Delta$, и тогда соответствующая коиндуктивная конструкция сразу даёт нам стандартное вероятностное пространство Ω вместе с измеримыми функциями на нём.

3.3 Канонические и неканонические конструкции

Отметим, что индуктивные и коиндуктивные конструкции, рассмотренные в **3.1**, являются примерами *канонических конструкций* в математике, поскольку они определяются своим универсальным свойством однозначно с точностью до канонического изоморфизма (или эквивалентности, если мы работаем в гомотопической теории типов). Мы хотим обсудить, насколько возможны и естественны неканонические конструкции,

и рассмотреть несколько примеров, часто используемых в математике, в частности, конструкцию алгебраического замыкания поля. Может ли быть такое, что только канонические конструкции обладают правом на существование?

3.3.1. (Выбор однозначно определенного объекта: ι-символ Гильберта.) Напомним, что мы обычно можем использовать в рассуждениях математические объекты, однозначно заданные с помощью некоторого свойства $P(x)$. Иначе говоря, если $P(x)$ — некоторый предикат (зависящий от предметной переменной x), и доказана теорема, что существует единственный x, для которого $P(x)$, то мы можем выбрать этот единственный x и использовать его дальше, как если бы он был задан явной конструкцией. Такой выбор обычно формализуется в логике с помощью ι-символа Гильберта, который делает из предиката (т.е. формулы со свободной переменной) $P(x)$ терм $\iota_x.P(x)$ (читается: «такой x, что $P(x)$» или «тот x, для которого $P(x)$»), который затем можно использовать внутри произвольных выражений. Это работает и в том случае, когда $P(x)$ зависит от дополнительных переменных: например, если доказано, что для любого y (из некоторой области или типа Y) существует единственный x, такой, что $P(x, y)$, то $\iota_x.P(x, y)$ является корректным термом (зависящим от y). Например, если $\theta : X \to Y$ — это некоторая функция, и мы доказали ее биективность, то $y \mapsto \iota_x.(\theta(x) = y)$ задает обратную функцию $\theta^{-1} : Y \to X$.

Хорошо известно, что если ι-символы используются внутри доказательства некоторого утверждения, в формулировке которого их нет, то можно формально исключить все ι-символы из доказательства с помощью простых преобразований. Грубо говоря, каждое вхождение $\iota_x.P(x, y)$ заменяется на новую свободную переменную x', и снаружи добавляется дополнительное условие $P(x', y)$. Это было доказано как раз еще Гильбертом и Бернайсом. Поэтому введение ι-символа совершенно безобидно и не приводит к каким-то фундаментальным изменениям в логике. В частности, ι-символ допустимо использовать в интуиционистской логике, семантике Крипке–Жуаяля, интуиционистской теории типов Мартин–Лёфа.

Следует отметить, что схожий τ-символ, который используется Бурбаки в основаниях теории множеств для определения кванторов и для формализации аксиомы выбора, вовсе не так безобиден. Напомним, что $\tau_x.P(x)$ можно использовать всегда; τ-символ каким-то образом выбира-

ет один из элементов, для которого $P(x)$ верно, если такие есть, причем если $P(x) \Leftrightarrow Q(x)$, то волшебным образом $\tau_x.P(x) = \tau_x.Q(x)$. Ясно, что, несмотря на то, что τ-символ на первый взгляд очень похож на ι-символ, в действительности он включает в себя аксиому выбора, и потому не может быть использован, например, в интуиционистской логике. Исключить τ-символ из доказательств, где он используется, тоже обычно нельзя. Например, с помощью τ-символа легко доказать, что любое сюръективное отображение множеств $f : X \to Y$ обладает сечением, а без τ-символа это, вообще говоря, неверно.[1]

3.3.2. (Категорный принцип выбора однозначно определенного объекта.) Принцип выбора однозначно определенного объекта обычно (неявно) распространяется и на теорию категорий, где разрешается выбирать один из объектов, заданных однозначно с точностью до однозначно определенного изоморфизма, или же одну из эквивалентных категорий, если все эти категории канонически эквивалентны. В действительности в теории категорий постоянно используется этот принцип, но почти всегда это происходит неявно.

3.3.3. (Гомотопический принцип выбора однозначно определенного объекта.) Если мы переходим к высшим категориям, и, в частности, к гомотопическим типам (которые, как известно, то же самое, что и ∞-группоиды), то мы получаем гомотопический принцип выбора однозначно определенного объекта: *если все способы выбора некоторого объекта образуют стягиваемое пространство, то можно считать это пространство точкой и зафиксировать выбор одного объекта.* Иначе говоря, в гомотопическом контексте существование и единственность означают непустоту и стягиваемость некоторого пространства. Отметим, что если пространство связно, но не стягиваемо, этот принцип не работает. Точно так же обычный категорный принцип однозначного выбора не работает в связных группоидах, в которых есть нетривиальные автоморфизмы объектов.

3.3.4. (Инициальные и финальные объекты в ∞-категориях, а также

[1] В действительности Гильберт определил не ι-символ, выбирающий объект, который существует и единственен, а ε-символ, близкий по своим свойствам к τ-символу Бурбаки и, в частности, не требующий единственности объекта с указанным свойством. Поэтому ε-символ не распространяется на интуиционистскую логику, в отличие от обсуждаемого выше ι-символа, по существу являющегося интуиционистской версией ε-символа.

пределы и копределы.) Отметим, что всевозможные варианты выбора инициального (или финального) объекта в ∞-категории $\mathcal{C}$ (в смысле J. Lurie) образуют стягиваемое пространство (если он вообще существует). Именно поэтому допустимо говорить об определенном инициальном или финальном объекте, как если бы он был единственным. Поскольку пределы и копределы диаграмм в ∞-категории $\mathcal{C}$ определяются как некоторые финальные или инициальные объекты в подходящих вспомогательных ∞-категориях, допустимо также говорить о конкретных пределах или копределах, как если бы они были единственными. В гомотопическом смысле они и есть единственные.

3.3.5. (Индуктивные и коиндуктивные конструкции в ∞-категориях и в гомотопической теории типов.) Аналогичным образом, поскольку индуктивные и коиндуктивные конструкции являются инициальными или финальными объектами в соответствующих категориях диаграмм, оказывается допустимым использовать их не только в обычных категориях и в интуиционистской теории типов Мартин-Лёфа, но и в их гомотопических аналогах — ∞-категориях и гомотопической теории типов.

В этом смысле индуктивные и коиндуктивные конструкции очень естественны (каноничны) и могут использоваться в математике практически в любых ситуациях.

3.3.6. (Зависимый однозначный выбор.) Отметим, что сформулированный выше принцип «гомотопического однозначного выбора» (если пространство непусто и стягиваемо, то можно выбрать из него элемент, как если бы оно было одноточечным) работает и в ситуациях, когда есть дополнительные параметры. Например, если Y — некоторый тип, и для каждого $y : Y$ (т.е. для каждого «элемента» y типа Y) задан тип $X(y)$, зависящий от y, то если доказано, что $X(y)$ стягиваемо для любого $y : Y$, то мы можем построить сечение $f : \prod_{(y:Y)} X(y)$ — иначе говоря, такую «функцию», заданную на Y, что $f(y) : X(y)$ для любого $y : Y$. Неформально это следует из того, что все слои проекции $p : X = \sum_{(y:Y)} X(y) \to Y$ стягиваемы, и потому пространство сечений f отображения p тоже стягиваемо, а значит, из него можно выбрать как бы единственный элемент.

Это соответствует тому, что мы говорили в **3.3.1** про ι-символ, зависящий от дополнительных параметров. Однако при формальном построении гомотопической теории типов для обоснования этой конструкции используется аксиома унивалентности. Вероятно, можно было бы

обойтись и введением гомотопического ι-символа.

Отметим, что строить сечения отображений, про которые неизвестно, что все их слои стягиваемы, вообще говоря, *нельзя*, даже если все слои непусты. В обычной математике мы привыкли обходить это ограничение с помощью аксиомы выбора, однако в гомотопическом мире даже аксиома выбора не помогает: если $p : X \to Y$ — расслоение топологических пространств, и Y — клеточный комплекс, то, вообще говоря, p не обладает непрерывным сечением, если только расслоение не является ацикличным. В качестве примера можно взять $X = \mathbb{R}$, $Y = \mathbb{R}/\mathbb{Z}$.

3.3.7. (Неканонические конструкции в математике.) Мы видим, что мы должны ограничиться использованием в математике только канонических конструкций, т.е. таких, которые задают нужный объект однозначно с точностью до канонического изоморфизма или эквивалентности (иначе говоря, пространство вариантов выбора объекта должно быть стягиваемым). Мы на самом деле уже обсуждали этот важный принцип в [AB1],**2.1.13**, где в качестве решения предлагалось использовать всю категорию (весь группоид, ∞-группоид или всё пространство) вариантов выбора, если эта категория не эквивалентна точечной.

Однако в математике есть важные конструкции, не являющиеся каноническими в этом смысле. Как быть с ними?

3.3.8. (Пример неканонической конструкции: алгебраическое замыкание поля.) Мы уже видели в [AB1],**2.1.13**, что важным примером неканонической конструкции является конструкция алгебраического замыкания произвольного поля k. Категория всех алгебраически замкнутых алгебраических расширений $k \hookrightarrow \Omega$ оказывается связным группоидом, но объекты этой категории обладают нетривиальными автоморфизмами, т.е. между двумя алгебраическими замыканиями поля k нет канонического изоморфизма.

В действительности можно видеть, что все общие конструкции алгебраического замыкания $\bar{k}$ задействуют аксиому выбора. Например, мы можем рассмотреть множество классов изоморфизмов конечных расширений $\{k \hookrightarrow K_\iota\}_{\iota \in I}$ (это вполне можно проделать конструктивно, поскольку конечномерные k-алгебры задаются конечным набором структурных констант, и мы можем выделить из всевозможных наборов сначала те, что задают ассоциативную коммутативную алгебру с единицей, а затем и те, что соответствуют полям, хотя для применения данной конструкции достаточно просто взять все ассоциативные коммутатив-

ные k-алгебры с единицей), затем строим их ограниченное тензорное произведение $A := \bigotimes'_{\iota\in I} K_\iota$ (оно является копроизведением в категории коммутативных k-алгебр и потому канонично), затем выбираем в A какой-нибудь максимальный идеал $\mathfrak{m}$ по теореме Крулля и полагаем $\bar{k} := A/\mathfrak{m}$. Ясно, что последний шаг — выбор максимального идеала по теореме Крулля — существенно использует аксиому выбора.

Интересно, что и доказательство того факта, что любые два алгебраических замыкания поля k изоморфны, также существенно задействует аксиому выбора, например, в виде леммы Цорна, примененной ко всевозможным подрасширениям одного алгебраического замыкания и их вложениям во второе алгебраическое замыкание. Либо можно снова профакторизовать тензорное произведение этих двух алгебраических замыканий по какому-нибудь максимальному идеалу (выбранному с помощью теоремы Крулля) и тем самым построить алгебраическое замыкание, изоморфное одновременно обоим исходным алгебраическим замыканиям.

Нужно выработать какое-то отношение к алгебраическому замыканию, исходя из этих фактов. Уже видно, что едва ли получится определить алгебраическое замыкание поля в рамках, например, гомотопической теории типов. Но что можно сделать? В [AB1],**2.1.13** мы предложили два варианта:

- Рассматривать весь связный группоид алгебраических замыканий поля k. Это почти эквивалентно тому, чтобы работать с одним алгебраическим замыканием $\bar{k}$, но использовать только $\mathrm{Gal}(\bar{k}/k)$-эквивариантные конструкции.

- Для конкретного поля k попытаться задать дополнительную структуру, делающую алгебраическое замыкание единственным. Например, можно строить поле алгебраических чисел $\bar{\mathbb{Q}}$ вместе с вложением $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

В связи с тем, что изоморфность двух различных алгебраических замыканий также оказывается неконструктивной и существенно использует аксиому выбора, возможно, надо рассмотреть еще один вариант:

- Использовать категорию всех конечных расширений поля k в качестве замены алгебраического замыкания $\bar{k}$.

По всей видимости, для произвольного поля k этот вариант является наилучшим. Однако для конкретных k у нас может быть выбор.

3.3.9. (Алгебраические замыкания $\bar{\mathbb{F}}_p$ и $\bar{\mathbb{Q}}_p$ менее каноничны, чем $\bar{\mathbb{Q}}$ и $\bar{\mathbb{R}} = \mathbb{C}$.) Интересным следствием предыдущих наблюдений является тот факт, что $\bar{\mathbb{R}} = \mathbb{C}$ оказывается каноничным (потому что $\mathbb{R}$ задается с помощью коиндуктивных конструкций, а затем $\mathbb{C}$ можно построить как $\mathbb{R} \times \mathbb{R}$; основную теорему алгебры можно доказать конструктивно), и потому $\bar{\mathbb{Q}}$, снабженное вложением $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, также канонично (мы можем построить $\bar{\mathbb{Q}}$ как множество алгебраических комплексных чисел). При этом, например, $\bar{\mathbb{F}}_p$ гораздо менее канонично. Тем более $\bar{\mathbb{Q}}_p$ неканонично.

Для того, чтобы понять это, посмотрим сначала на конечные расширения $\mathbb{F}_{p^n}$. Чтобы их построить, надо найти какой-нибудь неприводимый многочлен $P(X) \in \mathbb{F}_p[X]$ степени n и положить $\mathbb{F}_{p^n} := \mathbb{F}_p[X]/(P(X))$. Однако эта конструкция неканонична, поскольку неприводимых многочленов $P(X)$ много. Мы могли бы попытаться сделать эту конструкцию конструктивной, например, взяв лексикографически наименьший $P(X)$, но это не особо помогает (конструкция становится конструктивной, но все равно неканоничной), что становится заметно, когда мы пытаемся вложить $\mathbb{F}_{p^n}$ в $\mathbb{F}_{p^{nn'}}$ — возникает n' вариантов вложения, и непонятно, какой из них выбрать. Если мы выберем один из них каким-нибудь конструктивным, но неканоничным образом — например, выберем тот из них, что отображает выделенную образующую $\mathbb{F}_{p^n}$ в элемент $\mathbb{F}_{p^{nn'}}$ с лексикографически наименьшими координатами в выделенном базисе — то мы потом за это расплатимся, когда попытаемся вложить $\mathbb{F}_{p^n}$ и $\mathbb{F}_{p^{nn'}}$ в $\mathbb{F}_{p^{nn'n''}}$ и увидим, что получившийся треугольник вложений некоммутативен. А ведь для построения $\bar{\mathbb{F}}_p$ придется так делать, поскольку это индуктивный предел всех $\mathbb{F}_{p^n}$. Однако интересно, что в этом случае можно доказать существование согласованной системы вложений и как следствие их индуктивного предела — поля $\bar{\mathbb{F}}_p$, не используя аксиомы выбора. Например, можно последовательно строить вложения $\mathbb{F}_{p^{n!}} \hookrightarrow \mathbb{F}_{p^{(n+1)!}}$ и затем взять их индуктивный предел. Иначе говоря, алгебраическое замыкание $\bar{\mathbb{F}}_p$ всё же есть, и все варианты его выбора неканонически изоморфны, но зафиксировать один из них мы не можем.

Можно было бы попытаться изготовить более каноничную конструкцию $\mathbb{F}_{p^n}$ с помощью первообразных корней $(p^n - 1)$-ой степени из единицы, но это тоже не очень помогает, потому что корней из единицы слишком много и непонятно, как выбрать один из них.

3.3.10. (Пример: поля деления круга $\mathbb{Q}(\sqrt[n]{1})$ над $\mathbb{Q}$.) Отметим, что поля деления круга $\mathbb{Q}(\sqrt[n]{1})$ оказываются гораздо более каноничными, чем их

аналоги над $\mathbb{F}_p$. Это происходит из-за того, что многочлен деления круга $\Phi_n(X) := \prod_{d|n}(X^d-1)^{\mu(n/d)}$ конструктивен и неприводим над $\mathbb{Q}$, так что мы можем просто положить $\mathbb{Q}(\sqrt[n]{1}) := \mathbb{Q}[X]/(\Phi_n(X))$. Этот способ не работает над $\mathbb{F}_p$, потому что там $\Phi_n(X)$ не будет неприводим, и придется произвольным образом выбирать один из его сомножителей. Однако в действительности канонично не $\mathbb{Q}(\sqrt[n]{1})$, а $\mathbb{Q}(\sqrt[n]{1})$ вместе с фиксированным первообразным корнем из единицы ζ_n. Разница становится существенной, когда мы пытаемся построить $\mathbb{Q}^{ab} = \mathbb{Q}(\sqrt[\infty]{1}) = \varinjlim_n \mathbb{Q}(\sqrt[n]{1})$. Более-менее единственный систематический способ выбрать согласованную систему первообразных корней из единицы $\zeta_n \in \mathbb{Q}(\sqrt[n]{1})$ — это снова вложить всё в $\mathbb{C}$ и положить $\zeta_n := e^{2\pi i/n}$.

В итоге получается, что $\mathbb{Q}^{ab}$ как бы есть (нам не нужна аксиома выбора для построения изоморфизмов между его разными реализациями), но нам нужно либо вложить его в $\mathbb{C}$, либо использовать только конструкции, эквивариантные относительно $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \hat{\mathbb{Z}}^*$.

3.3.11. ($\bar{\mathbb{F}}_p$ как факторкольцо $\mathbb{Z}^{cycl} \subset \mathbb{Q}^{ab} \subset \mathbb{C}$.) Поскольку поля деления круга над $\mathbb{Q}$ оказываются конструктивны, если зафиксировать их вложения в $\mathbb{C}$, возникает соблазн воспользоваться этим для построения $\bar{\mathbb{F}}_p$. А именно, рассмотрим целое замыкание $\mathbb{Z}^{cycl} \subset \mathbb{Q}^{ab} \subset \mathbb{C}$ (оно вполне конструктивно и канонично как подкольцо $\mathbb{C}$), затем выберем какой-нибудь простой идеал $\mathfrak{p}$ над p и положим $\bar{\mathbb{F}}_p := \mathbb{Z}^{cycl}/\mathfrak{p}$. Проблема снова в том, что у нас нет канонического способа выбора максимального идеала $\mathfrak{p}$. В данном случае можно обойтись без теоремы Крулля и аксиомы выбора, проделав счётную последовательность произвольных выборов из конечных множеств, но по существу эта та же проблема, что и при прямом построении $\bar{\mathbb{F}}_p$: надо каким-то образом выбрать из неприводимых сомножителей $\Phi_n(X)$ по модулю p один, и непонятно, как это сделать канонически.

3.3.12. (Конструктивность и каноничность.) Предыдущие примеры показывают, что конструктивность и каноничность вовсе не одно и то же. Например, конструкция $\mathbb{F}_{p^n}$ с помощью лексикографически наименьшего неприводимого многочлена степени n над $\mathbb{F}_p$ конструктивна, но не канонична. С другой стороны, каноническая конструкция не обязана быть конструктивной: если мы докажем, что некоторый объект существует и единствен (в подходящем смысле), но не приведем явной конструкции, мы все же считаем себя вправе выбрать его с помощью ι-символа Гильберта.

3.3.13. (Следует ли отказаться от всех неканоничных конструкций?) Возникает вопрос: следует ли отказаться от неканоничных конструкций вообще, раз уж они зачастую используют аксиому выбора и потому произвольны, и к тому же не могут быть перенесены в гомотопическую теорию типов, которая претендует на роль новых, более правильных, оснований математики?

Мы считаем, что такой радикальный подход был бы слишком преждевременен. Неканоничные конструкции, такие, как алгебраическое замыкание поля, позволяют нам относительно легко доказывать содержательные математические факты. Очень может быть, что эти факты могут быть доказаны более канонично — например, с использованием категории всех конечных расширений поля k вместо его алгебраического замыкания. Однако подобные доказательства наверняка окажутся длиннее и сложнее, и потому более запутанными и менее понятными. В конце концов, программа переписывания всей математики в рамках гомотопической теории типов продвинулась не слишком далеко, вероятно, как раз поэтому.

Однако что мы можем сделать, так это лучше отдавать себе отчёт в том, какие конструкции каноничны, а какие нет, и если мы все же осознанно используем неканонические конструкции — то в каком виде их использование наиболее естественно. Так, если уж мы используем алгебраическое замыкание $\bar{k}$, мы должны заботиться о том, чтобы все наши построения были эквивариантны относительно группы Галуа, или, что одно и то же, чтобы было неважно, какое именно алгебраическое замыкание мы выбрали, и каким именно образом два алгебраических замыкания изоморфны друг другу. Такого рода общие принципы позволяют быстро отсекать попытки неправильного использования неканонических объектов, раз уж мы не готовы совсем избавиться от них.

Список литературы

[GHS] Svante Janson, *Gaussian Hilbert spaces*, Cambridge Tracts in Mathematics **129**, Cambridge University Press, 1997.

[DS] Alexander S. Kechris, *Classical descriptive set theory*, Graduate Texts in Mathematics **156**, Springer-Verlag, 1995.

[TG] Nicolas Bourbaki, *Topologie Générale*, Hermann, Paris, 1971 (chap. 1–4), 1974 (chap. 5–10).

[OP] Gabor Szegö, *Orthogonal polynomials*, AMS, 1978.

[TT] Peter Johnstone, *On a topological topos*, Proc. London Math. Soc. (3) **38** (1979) pp. 237–271.

[CH1] Th. Coquand, G. Huet, *Constructions: A higher order proof system for mechanizing mathematics.* In EUROCAL'85, volume **203**, Linz, 1985. Springer-Verlag.

[CH2] Th. Coquand, G. Huet, *The Calculus of Constructions,* Information and Computation, **76** (2/3), 1988.

[CP] Th. Coquand, C. Paulin-Mohring. *Inductively defined types,* in P. Martin-Löf and G. Mints, editors, Proceedings of Colog'88, **417**. Springer-Verlag, 1990.

[SP] Thierry de la Rue, *Espaces de Lebesgue*, Séminaire de Probabilités XXVII, Lecture Notes in Mathematics **1557**, Springer, 1993, pp. 15–21.

[DF] Bruno de Finetti, *La prévision: ses lois logiques, ses sources subjectives*, Annales de l'institut Henri Poincaré, **7** (1937) no. 1, pp. 1–68.

[AB1] Дуров Н.В., *Обзор подходов построения абсолютной геометрии*, Препринт ПОМИ 8 (2022).

[AB3] Дуров Н.В., *Индуктивные и коиндуктивные конструкции в математике*, Препринт ПОМИ 9 (2022).

[AB4] Дуров Н.В., *Примеры эффективных систем счисления*, Препринт ПОМИ 10 (2022).

[AB5] Дуров Н.В., *Вероятностные свойства избыточных систем счисления*, Препринт ПОМИ 11 (2022).

[AB6] Дуров Н.В., *Регулярные пространства и регулярные отображения*, Препринт ПОМИ 12 (2022).