Математические структуры и моделирование
2009, вып. 19, с. 28–44

УДК 512.581:510.5

ЭФФЕКТИВНЫЙ ТОПОС КАК СИНТЕТИЧЕСКАЯ ВСЕЛЕННАЯ ДЛЯ ТЕОРИИ ВЫЧИСЛЕНИЙ

Е.О. Хлызов

В статье обсуждается применение теории элементарных топосов Ловера к теории вычислимости. Дается пример построения синтетической теории вычислений на основе так называемого эффективного топоса.

Краткое вступление

Предположим, некий математик собрался изучить вполне определенный вид математических структур, таких, как, например, топологические пространства в паре с непрерывными отображениями или эффективно построимые множества в совокупности с эффективно вычислимыми функциями. Для выделения указанных объектов математик следует классическому пути, рассматривая множества, наделенные дополнительной структурой и отображения, сохраняющие эту структурур. Тогда можно говорить о том, что он изучает топологию и теорию вычислений. Но есть и другой путь – изолировать изучаемые объекты, поместив их в некоторую синтетическую вселенную, в которой специфическая структура объекта является всеобщей, т.е. распространяющейся на всю вселенную. Таким образом, мы получаем синтетический мир с некоторой заданной в нем логикой (не обязательно классической). Находящийся в этом мире математик, со своей точки зрения, изучает простые множества и простые отображения, а с точки зрения внешнего наблюдателя, изучает строго определенный класс множеств и отображения, позволяющие остаться в рамках этого класса. Такой подход принято называть синтетическим.

Автор рассматривает данную статью как попытку в максимально простой форме, на примере теории вычислимости, показать возможности использования топосов в качестве синтетических вселенных. В ней рассматривается пример построения синтетической теории вычислений на основе так называемого *эффективного топоса.*

Омский государственный университет им. Ф.М. Достоевского.
E-mail: hlyzov@gmail.com

1. Используемые обозначения

Функцию, отображающую заданное множество на множество всех его подмножеств, будем обозначать $\mathcal{P}$. Под A^B подразумевается множество всех функций из B в A. Обозначение ! для стрелки отражает факт ее единственности. Для выражения «$S1$ такое, что $S2$» будет использоваться сокращение «$S1.S2$». Истина и ложь обозначаются знаками $\perp$ ($false$) и $\top$ ($true$) соответственно. Объяснения остальных обозначений будут даны по ходу изложения материала.

2. Начальные определения

Для понимания следующих параграфов от читателя потребуется знание основных определений теории категорий. Далее приводится необходимый минимум, для того чтобы подойти к понятию элементарного топоса. Для более детального ознакомления с теорией категорий и теорией топосов рекомендуется обратиться к соответствующей литературе (см., например, [1–3]).

Определение 1. Категория $\mathcal{C}$ включает в себя:

1. Коллекцию **объектов** $Ob(\mathcal{C})$.

2. Коллекцию **морфизмов** (*стрелок*) $Mor(\mathcal{C})$.

3. Две операции $dom, cod : Mor(\mathcal{C}) \to Ob(\mathcal{C})$, сопоставляющие каждому морфизму f два объекта, называемые, соответственно, **областью определения** (*доменом*) и **областью значений** (*кодоменом*) морфизма f.

4. Оператор композиции $\circ : Mor(\mathcal{C}) \times Mor(\mathcal{C}) \to Mor(\mathcal{C})$, сопоставляющий каждой паре морфизмов $\langle f, g\rangle$, таких, что $dom(g) = cod(f)$ морфизм $g \circ f : dom(f) \to cod(g)$, таким образом, что выполняется **закон ассоциативности**:

$$h \circ (f \circ g) = (h \circ f) \circ g.$$

5. Оператор $id : Ob(\mathcal{C}) \to Mor(\mathcal{C})$, сопоставляющий каждому объекту A, тождественный морфизм $id_A : A \to A$, таким образом, что выполняется **закон единицы**:

$$id_B \circ f = f = f \circ id_A.$$

Примеры категорий:

1. **Set** – объекты: множества, стрелки: все функции между множествами.

2. **Top** – объекты: топологические пространства, стрелки: все непрерывные функции.

3. **N** – объект: N (единственный), стрелки: отображения из N в N. Каждая стрелка представляет собой натуральное число ($c = m \circ n = m + n \in Mor(\mathbf{N}), \forall m, n \in Mor(\mathbf{N})$).

Определение 2 (Декартово замкнутая категория)**.** Категория $\mathcal{C}$ декартово замкнута, если она:

1. Содержит терминальный объект, т.е. объект, к которому каждый объект категории имеет единственную стрелку, иначе говоря, утверждается, что: $\exists\ \mathbf{1} \in Ob(\mathcal{C})\ .\ \forall X \in Ob(\mathcal{C})\ \exists! f \in Mor(\mathcal{C})\ .\ cod(f) = \mathbf{1}, dom(f) = X$. В категории Set примером терминального объекта является множество с одним элементом.

2. Для любых двух объектов $X, Y \in Ob(\mathcal{C})$ существует объект $X \times Y \in Ob(\mathcal{C})$, который, вместе с двумя стрелками $pr_X : X \times Y \to X$, $pr_Y : X \times Y \to Y$, обладает следующим свойством: для произвольной пары стрелок $f : C \to X$, $g : C \to Y$ существует единственная стрелка $h : C \to X \times Y$, такая, что следующая диаграмма коммутативна:

$$\begin{tikzcd} & C \arrow[dl, "f"'] \arrow[d, dashed, "h"'] \arrow[dr, "g"] & \\ X & X \times Y \arrow[l, "pr_X"'] \arrow[r, "pr_Y"] & Y \end{tikzcd}$$

   Тройку $< X \times Y, pr_X, pr_Y >$ называют **категорным произведением** X и Y, а стрелки pr_X и pr_Y называют **проекциями**. В категории Set категорным произведением является прямое произведение двух множеств.

3. Категория допускает **экспоненцирование**, т.е. для любых двух объектов $X, Y \in Ob(\mathcal{C})$ существует объект $Y^X \in Ob(\mathcal{C})$, называемый экспоненциалом, и специальная стрелка $ev : Y^X \times X \to Y$, называемая **функцией значения**, такие, что для любого объекта $Z \in Ob(\mathcal{C})$ и любой стрелки $g : Z \times X \to Y$ существует единственная стрелка $\hat{g} : Z \to Y^X$, такая, что следующая диаграмма коммутативна:

$$\begin{tikzcd} Y^X \times X \arrow[dr, "ev"] & \\ Z \times X \arrow[u, dashed, "\hat{g} \times 1_X"] \arrow[r, "g"'] & Y \end{tikzcd}$$

   В категории Set экспоненциалом Y^X является множество всех функций из X в Y, а функцией значения – отображение, переводящее пару ($f \in Y^X, X$) в множество $f(X)$.

Определение 3 (Классификатор подобъектов)**.** Говорят, что категория $\mathcal{C}$ с терминальным объектом **1** имеет **классификатор подобъектов** Ω, если существует единственная стрелка $\top : \mathbf{1} \to \Omega$ и выполняется следующее правило (Ω-аксиома):

Для каждого инъективного отображения (монострелки) $f : A \to B$ существует единственная $\chi_A : B \to \Omega$, такая, что: $\top \circ ! = \chi_f \circ f$. На языке теории категорий предыдущее выражение формулируется в виде утверждения, что следующая диаграмма **коммутативна** (коммутативные квадраты принято называть *декартовыми*):

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[d, "!"'] & d \arrow[d, "\chi_A"] \\ \mathbf{1} \arrow[r, "\top"'] & \Omega \end{tikzcd}$$

Стрелку χ_A при этом называют **характеристической** стрелкой для A. В категории Set, Ω имеет вид $\{0{,}1\}$, а характеристическая функция для подмножества $A \subset B$ определяется следующим образом:

$$\chi_A(x) = \begin{cases} 1, & x \in A; \\ 0, & x \notin A. \end{cases}$$

Наконец мы подошли к наиболее интересующему нас понятию топоса. Следующее определение эквивалентно данному В. Ловером и М. Тирни в 1969 году:

Определение 4 (Топос)**.** Декартово замкнутая категория с классификатором подобъектов называется ***элементарным топосом***.

Слово «элементарный» лишь указывает на природу данного топоса, а точнее, на ее отличие от известного до него **топоса Гротендика** и в дальнейшем будет опускаться.

К сожалению, без полноценного введения в теорию категорий сложно привести примеры топосов отличных от Set. Поэтому ограничимся простейшими топосами, так или иначе образованными от Set:

1. Самым естественным примером топоса является сама категория Set (вообще, топос можно мыслить как некоторое обобщение Set). В определениях выше именно эта категория была использована в качестве наглядного пособия.

2. Категория Finset является подкатегорией категории Set и в качестве объектов содержит конечные множества. Finset также является топосом – экспоненциал, классификатор и категорное произведение строятся так же, как в Set.

3. Категория пучков множеств в топологическом пространстве является топосом [5]. Вообще, категория множеств является топосом, как категория пучков множеств одноточеченого пространства.

Более сложный пример топоса, позволяющего работать с «эффективно конструируемыми» множествами и «эффективно вычислимыми» отображениями, будет рассмотрен чуть позже. Топосы интересеы тем, что они могут выступать в качестве описанной в начале статьи синтетической вселенной. Впервые такие эксперименты были проведены Ловером, что привело к созданию синтетической дифференциальной геометрии [9, 10].

3. Зарождение синтетической теории вычислимости

В связи с тем, что каждый топос определяет собственное логическое исчисление [2], упоминание о синтетической теории вычислимости (СТВ) можно встретить еще в 1986 г. [12], т.е. практически одновременно с появлентем **эффективного** и **рекурсивного** топосов. В то время СТВ не получила значимого развития и «категорификация» приближалась к теории вычислений посредством *синтетической теории доменов* – теории, где применение синтетического подхода позволило получить многообещающие результаты [6, 13]. В 2005 году словенский математик Андрей Бауер выступил с докладом «Первые шаги в синтетической теории вычислимости», где была сделана попытка определить начальные положения новой теории, опираясь на уже довольно богатый опыт наработок с вычислениями в категориях. В качестве модели он предпочел использовать эффективный топос *Eff*, описанный М. Хиландом в [8]. Интересно, что *Eff* является элементарным топосом, но не является топосом Гротендика в отличие от своего «конкурента» – рекурсивного топоса [12]. Далее мы «вскроем» СТВ, предложенную Бауером и разберем строение *Eff*.

4. Строение категории *Eff*

Рассмотрим новую категорию «предпорядок», определенную тем, что для любых двух ее объектов $X, Y \in P$ существует не более одного морфизма $f : X \to Y$. На множестве объектов P (в случае, когда можно говорить о совокупности объектов именно как о множестве, т.е. категория P **мала**) можно задать отношение предпорядка следующим образом: $X \leq Y \iff \exists f : X \to Y$.

Следующее определение, которое понадобится далее, относится к категорным построениям и получается путем обращения всех стрелок в определении категорного произведения.

Определение 5 (Копроизведение)**.** Копроизведением двух объектов $X, Y \in Ob(\mathcal{C})$ называется объект $X+Y \in Ob(\mathcal{C})$, который вместе с двумя стрелками $i_X : X \to X+Y$, $i_Y : Y \to X+Y$, обладает следующим свойством: для произвольной пары стрелок $f : X \to C$, $g : Y \to C$ существует единственная стрелка $h :$

$X+Y \to C$, такая, что следующая диаграмма коммутативна:

$$\begin{tikzcd} & C & \\ X \arrow[ur, "f"] \arrow[r, "i_X"] & X+Y \arrow[u, dashed, "h"] & Y \arrow[ul, "g"'] \arrow[l, "i_Y"'] \end{tikzcd}$$

Тройку $< X+Y, i_X, i_Y >$называют **категорным копроизведением** или **суммой** X и Y, а стрелки i_X и i_Y называют **инъекциями**. В категории Set категорным произведением является прямое произведение двух множеств.

Для построения *Eff* нужна алгебра более общая чем алгебра Гейтинга (которая определяется на частично упорядоченных множествах), но имеющая схожие свойства. Заменой отношения частичного порядка на отношение предпорятка получаем следующее определение.

Определение 6. Предалгебра Гейтинга H – это декартово замкнутая категория предпорядка с произведениями ($\wedge$), копроизведениями ($\vee$), начальным объектом $\perp$, конечным объектом $\top$ и экспоненциалом ($\to$). Под $p \equiv q$ подразумевается, что $p \leq q$ и $q \leq p$.

Легко проверить, что предалгебра Гейтинга является интерпретацией конструктивной логики высказываний [11]. Конструктивность можно мыслить как необходимость «подтверждать» абстрактные выводы, т.е. для каждого такого вывода должен предъявляться эффективный алгоритм вычисления результата. В конструктивной логике высказывание ($A \vee !A$) недоказуемо; чтобы понять почему, достаточно представить себе множество «точек останова» $K \subset \mathbb{N}$. Если конструктивной истиной было бы высказывание $n \in K \vee n \notin K$, то это означало бы, что существует алгоритм, который, будучи примененным на натуральное число n, сообщил бы, входит ли n в K или нет. Но, согласно тезису Черча, такого алгоритма не существует.

Определение 7. Пусть X – некоторое множество, тогда мы можем превратить степенное множество $\mathcal{P}(\mathbb{N})$ в предалгебру Гейтинга следующим способом:

Если $F, G \in (\mathcal{P}(\mathbb{N}))^X$ таким образом, что $F(x), G(x) \subseteq \mathbb{N}$ для кажого $x \in X$, то:

$$\begin{gathered} (F \wedge G)(x) = F(x) \wedge G(x) \\ (F \vee G)(x) = F(x) \vee G(x) \\ (F \to G)(x) = F(x) \to G(x) \end{gathered}$$

И $F \leq G \iff \bigcap\limits_{x \in X} F(x) \to G(x) \neq \varnothing$.

Мы будем писать также $\mathcal{P}(\mathbb{N}) \vDash (F \leftrightarrow G)$ для обозначения $\mathcal{P}(\mathbb{N}) \vDash (F \to G) \wedge (G \to F)$.

Определение 8. Пусть $F \in (\mathcal{P}(\mathbb{N}))^X$, если выполняется $\bigcap_{x \in X} F(x) \neq \varnothing$, то будем это записывать как $\mathcal{P}(\mathbb{N}) \vDash F$, а выполнение $F = \lambda x.F(x)$ будем записывать как $\mathcal{P}(\mathbb{N}) \vDash F(x)$.

Теперь можно перейти непосредственно к описанию элементов категории *Eff*. Доказательство единственной в этом параграфе теоремы (а также многих других, не вошедших в данную статью) можно посмотреть в соответствующей монографии [8].

Определение 9 (Объект *Eff*)**. Объект** $(X, =)$ в *Eff* – это множество X вместе с отношением эквивалентности в $\mathcal{P}(\mathbb{N})$, т.е. для каждых $x, x' \in X$ подмножество $|x = x'| \subseteq \mathbf{N}$ реализуемо симметрично и транзитивно, что означает:

$$\mathcal{P}(\mathbb{N}) \vDash |x = x'| \to |x' = x| \text{ и}$$
$$\mathcal{P}(\mathbb{N}) \vDash (|x = x'| \wedge |x' = x''|) \to |x = x''|.$$

Пусть $x \in X$, будем писать Ex для обозначения $|\mathrm{x} = \mathrm{x}|$.

Определение 10 (Функциональное отношение в *Eff*)**.** Пусть $(X, =), (Y, =) \in Ob(\mathit{Eff})$, тогда функциональное отношение из $(X, =)$ в $(Y, =)$ – это отображение $F : X \times Y \to \mathcal{P}(\mathbb{N})$, такое, что

- $\mathcal{P}(\mathbb{N}) \vDash (F(x, y) \wedge (|x = x'| \wedge |y = y'|)) \to F(x', y')$
- $\mathcal{P}(\mathbb{N}) \vDash F(x, y) \to (Ex \wedge Ey)$
- $\mathcal{P}(\mathbb{N}) \vDash F(x, y) \wedge F(x, y') \to |y = y'|$
- $\mathcal{P}(\mathbb{N}) \vDash Ex \to \{\langle k, m \rangle \,| k \in Ey \ \ y \in Y \ \ m \in F(x, y)\}$,

два функциональных отношения F, F' **эквивалентны** $(F \sim F')$, если

$$\mathcal{P}(\mathbb{N}) \vDash (F(x, y) \longleftrightarrow F'(x, y)).$$

Определение 11 (Тождественность в *Eff*)**.** Тождественное функциональное отношение в *Eff* из $(X, =)$ в $(X, =)$ определяется как $I(x, x') = |x = x'|$.

Определение 12 (Морфизм *Eff*)**. Морфизм**(стрелка) $f : (X, =) \to (Y, =)$ в *Eff* – это класс эквивалентности функциональных отношений $f = [F]$, где F – функциональное отношение, задающее f.

Теорема 1 (Хайланд)**.** *Eff – топос.*

Для лучшего уяснения внутреннего строения эффективного топоса рекомендуется обратиться к соответствующей литературе [8, 11, 12]. Далее, чтобы избежать серьезного углубления в теорию топосов (беря пример с Бауера), будет использоваться специальный внутренний язык. Внешнее описание *Eff* было дано выше, внутренне же топос можно представить как конструктивную теорию множеств, расширенную несколькими аксиомами, касающимися множеств и последовательностей натуральных чисел [4, 7].

5. Введение в Синтетическую теорию вычислений

В качестве одной из причин возникновения СТВ можно указать некоторую обособленность теории вычислений от остальной математики. Описания различных машин Тьюринга, числа Геделя, лямбда-абстракции придают ей некоторую особенность, но в то же время поднимают порог вхождения, требуя от математика знания результатов, полученных при использовании той или иной модели вычислений. СТВ позволяет работать с гораздо более привычными объектами – множествами и отображениями между ними, скрывая детали за высоким уровнем абстракции с помощью «внутреннего» языка родительского топоса. Поскольку в данном случае в качестве фреймворка используется топос *Eff* и одна из аксиом СТВ противоречит закону исключенного третьего в классической логике, мы будем работать в интуиционистской (конструктивной) логике. Наша цель на данном этапе – перенести некоторые понятия и теоремы классической теории на внутренний язык *Eff*, не выходя далеко за пределы конструктивной теории множеств. Следует также отметить, что в *Eff* вычислимость является встроенной, т.е. все, что выводимо в *Eff*, по определению имеет эффективный алгоритм для вычисления. Дальнейший текст является в большей степени обзорным, предложения и теоремы приводятся без доказательства. Для более полного ознакомления следует обратиться к [4].

То, что мы работаем в интуиционистской логике (ИЛ), означает, что мы будем иметь дело с выражениями, выходящими за рамки «классического» понимания. Помимо закона исключенного третьего, следующие общепринятые формулы также не верны (в общем) в ИЛ:

1. $\neg\neg\varphi \Longrightarrow \varphi$
2. $\neg\varphi \vee \neg\neg\varphi$
3. $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$
4. $\neg(\neg\varphi \wedge \neg\psi) \Longrightarrow \varphi \vee \psi$

В частности, это означает, что в интуиционистском смысле существуют аргументы, на которых ни одна из выше приведенных формул не выполняется. Отдельного параграфа заслуживает аксиома выбора.

6. Строение множеств

Для определения упорядоченной пары (элемент множества $A \times B$) мы рассмотрим операцию $\langle -, - \rangle$ вместе с проекциями π_1 и π_2, удовлетворяющих акиомам: $\pi_1 \langle x, y \rangle = x$ и $\pi_2 \langle x, y \rangle = y$. Определим понятия суммы и произведения семейства множеств $\mathcal{F} \subseteq \mathcal{P}(A)$:

$$\cup\mathcal{F} = \{x \in A | \exists S \in \mathcal{F}. x \in S\} \cap \mathcal{F} = \{x \in A | \forall S \in \mathcal{F}. x \in S\}.$$

Теперь мы готовы для следующего важного опредения:

Определение 13 (Натуральные числа)**.** Множество $\mathbb{N}$ вместе с элементом $0 \in \mathbb{N}$, называющимся *нулем*, и с функцией *выбора следующего элемента* $succ : \mathbb{N} \to \mathbb{N}$, такой, что для каждого множества A, $x \in A$ и $f : A \to A$ существует единственная функция $h : \mathbb{N} \to A$, такая, что $h(0) = x$ и $h(succ(n)) = f(h(n)$. Будем говорить, что функция h задана **простой рекурсией**. Одноэлементное множество $\mathbf{1}$ определяется как $\mathbf{1} = \{n \in \mathbb{N} | n = 0\}$. А пустое множество $\emptyset$ как $\emptyset = \{x \in \mathbf{1} | \bot\}$.

7. Строение функций

Граф $\Gamma(f)$ функции $f : A \to B$ – это отношение $\Gamma(f) \subseteq A \times B$, определенное для $x \in A, y \in B$ следующим образом:

$$(x, y) \in \Gamma(f) \iff f(x) = y.$$

Легко проверить, что граф является функциональным отношением. Наоборот, каждое функциональное отношение определяет функцию. Это известно как *аксиома единственного выбора*:

$$\forall R \in A \times B.((\forall x \in A.\exists! y \in B.R(x, y)) \implies \exists f \in B^A.\forall x \in A.R(x, f(x))).$$

Приведенная аксиома оказывается полезной при задании функций. Например, единичная функция $\mathbf{1}_A$ определяется как функция, чей граф является отношением равенства на A.

Теперь имеется достаточно инструментов для того, чтобы приступить к описанию теории. Прежде чем перейти к рассмотрению основных аксиом СТВ, определим понятие *разрешимости*. Для начала посмотрим на понятие истинностного значения в контексте ИЛ. Напомним, что истинностным значением называется высказывание без свободных переменных (например, $\top$, $\bot$, $\forall x \in (R).(x = 0 \vee x \neq 0)$).

Определение 14 (Множество истинностных значений)**.** $\Omega = P\mathbf{1}$.

В классической логике показывается, что только $\bot$ (ложь) и $\top$ (истина) являются элементами Ω (в некотором роде это просто форма закона исключенного третьего). В интуиционистской логике это утверждение неверно. Впрочем, это **не** означает, что Ω состоит более чем из двух элементов... Для того, чтобы это понять, следует вспомнить, что означает высказывание «множество имеет два элемента»: если $x, y \in A$, такие, что $x \neq y$ и не существует элемента $z \in A$, такого, что $z \neq x$ и $z \neq y$ – говорят, что множество A имеет два элемента в *слабом смысле*. С другой стороны, если при заданных условиях для любого элемента $z \in A$ верно, что либо $z = x$, либо $z = x$, говорят, что множество A имеет два элемента в сильном смысле. Таким образом, Ω имеет два элемента ($\bot$ и $\top$) в слабом смысле, но доказать, что Ω имеет два элемента в строгом смысле, мы можем только в рамках классической логики.

Ω является предалгеброй Гейтинга [1]. Таким образом, $p \wedge q \implies\iff p \implies$

[1]На самом деле, как показательное множество, Ω является полной алгеброй Гейтинга.

$(q \implies r)$. Отрицание является псевдодополнением, т.е. $\neg p$ определяется как наибольший элемент q, такой, что $p \wedge q = \perp$. Рассмотрим подмножество Ω, имеющее отношение к классической логике, элементы которого *разрешимы*, т.е. удовлетворяют закону исключенного третьего.

Определение 15 (Множество разрешимых истинностных значений).
$$\mathbf{2} = \{p \in \Omega | p \vee \neg p\}.$$

$\mathbf{2}$ имеет ровно два элемента в строгом смысле и вместе с операциями $\wedge$ и $\vee$ является булевой алгеброй.

Представим еще одно подмножество Ω, имеющее непосредственное отношение к классической логике.

Определение 16 (Классическое множество истинностных значений).
$$\Omega_{\neg\neg} = \{p \in \Omega | \neg\neg p \implies p\}.$$

Элементами $\Omega_{\neg\neg}$ являются истинностные значения, чья истинность может быть доказана «от противного» – если $\neg p$ ложно, значит p истинно. Дальше в тексте элементы $\Omega_{\neg\neg}$ будут называться «классическими». $\Omega_{\neg\neg}$ помимо того, что, как и Ω, является полной алгеброй Гейтинга, также является полной булевой алгеброй.

Приведенные множества соотносятся следующим образом:

$$\mathbf{2} \subseteq \Omega_{\neg\neg} \subseteq \Omega.$$

Более полную информацию можно будет получить позднее, когда добавится третье подмножество $\Sigma \subseteq \Omega$, играющее ключевую роль в СТВ.

8. Предикаты

Предикат $P \subseteq A$ может быть задан характеристической функцией $\chi_P : A \to \Omega$, определенной следующим образом:

$$\chi_P(x) = \{t \in \mathbf{1} | x \in P\}.$$

Наоборот, функция $\xi : A \to \Omega$ соотносится с подмножеством

$$\{x \in A |\ \xi(x) = \top\} \in A.$$

Таким образом, установлено биективное соответствие между предикатами на A, подмножествами A и пропозициональными функциями $A \to \Omega$. Пропозициональные функции, отображающие на подмножества Ω, приводят к особым видам предикатов. Например, функция $p : A \to \mathbf{2}$ представляет подмножество $S = \{x \in A |\ p(x) = \top\}$, такое, что $\forall x \in A.(x \in S \vee x \notin S)$. Такие предикаты и подмножества называются *разрешимыми*.

Если равенство на множестве задано вычислимым предикатом $(\forall x \in A.(x = y \vee x \neq y))$, то такое множество называется вычислимым.

Предложение 1. *Следующие множества разрешимы: натуральные числа, подмножества разрешимого множества, декартово произведение и сумма разрешимых множеств.*

9. Аксиомы СТВ

Определение 17 (Проективное множество)**.** Говорят, что два множества A, B *допускают выбор* (обозн. $AC(AB)$), если для каждого тотального отношения между A и B выполняется

$$\forall R \subseteq A \times B.((\forall x \in A.\exists y \in B.R(x, y)) \Longrightarrow \exists f \in B^A.\forall x \in A.R(x, f(x))).$$

Множество называется проективным, если $AC(A, B)$ выполняется для каждого множества B.

В классической теории множеств аксиома выбора утверждает, что все множества проективны. В нашем случае мы ограничены гораздо более серьезно, потому что в вычислительном смысле проективными являются только множества, каждый элемент которых имеет канонический код Геделя. Таким образом, можно ожидать, что множество $\mathbb{N}$ проективно, а множество $\mathbb{N}^{\mathbb{N}}$ – нет, потому что в последнем случае нельзя эффективным образом указать процедуру выбора канонического кода.

В конструктивной математике множество натуральных чисел, несомненно, должно быть проективно. Это уставнавливает следующая аксиома.

Аксиома 1 (Выбора числа)**.** *Множество натуральных чисел* $\mathbb{N}$ *проективно.*

Также понадобится следующее обобщение аксиомы выбора числа.

Аксиома 2 (Обусловленный выбор)**.** *Если R тотальное отношение на A и $x \in A$, тогда существует $f : \mathbb{N} \to A$, такое, что $f(0) = x$ и $R(f(n), f(n+1))$ выполняется для всех $n \in \mathbb{N}$.*

Третья аксиома выбора одновременно является и первой аксиомой СТВ. В конструктивной математике (по Бишопу) она в общем не принимается. Ее обоснование лежит на рассмотрении вычислительного аспекта классических подмножеств. Членство в классическом подмножестве $S \subseteq A$ проективного множества не несет никакой вычислительной нагрузки, таким образом, коды Геделя для элементов A кодируют ту же информациюю, что и для элементов S. Таким образом, мы можем использовать те же коды для множества и его подмножества, а раз элементы A имеют канонические коды, то, значит, элементы S также будут их иметь.

Аксиома 3 (Проективности)**.** *Классическое подмножество проективного множества проективно.*

10. Счетные и полусчетные множества

Вычислимые счетные множества играют центральную роль в классической теории вычислений. В СТВ они сохраняют свою значимость, только внутри *Eff* они выглядят как обычные счетные множества.

Определение 18. Множество A счетно (перечислимо), если существует сюрьективное отображение $e : \mathbb{N} \to \mathbf{1} + A$, называемое нумерацией A. Нумерация называется нумерацией без повторений, если $\forall n, m \in \mathbb{N}, e(n) = e(m) \Rightarrow n = m$.

Предложение 2. *Множество может быть пронумеровано без повторений тогда и только тогда, когда оно счетно и разрешимо.*

Следствие 1.1. *Каждое счетное подмножество* (N) *может быть пронумеровано без повторений.*

Ниже представлены некоторые утверждения касательно способов создания счетных множеств.

1. Декартово произведение двух счетных множеств счетно.
2. Объединение счетного семейства множеств счетно.
3. Пересечение двух счетных подмножеств разрешимого множества счетно.
4. Разрешимое подмножество счетного подмножества счетно.
5. Конечная последовательность счетных множеств формирует счетное множество.

Определенный интерес представляет собой множество всех счетных подмножеств $\mathbb{N}$, будем обозначать его $\mathcal{E}$:

$$\mathcal{E} = \{A = \mathcal{P}\mathbb{N} | A \ \}.$$

С этим множеством связана следующая любопытная теорема, показывающая, что $\mathcal{E}$ является дискретной топологией на $\mathbf{N}$.

Теорема 2. *Семейство* (E) *– это наименьшее из семейств* $(F) \subseteq \mathcal{P}(\mathbb{N})$*, таких, что:*

1. $0 \in (F)$ *и* $\mathbf{N} \in \mathcal{F}$.
2. $\{n\} \in \mathcal{F}$*для каждого* $n \in \mathbf{N}$.
3. *Если* $A, B \in \mathcal{F}$ *то* $A \cap B \in \mathcal{F}$.
4. *Если* $\mathcal{A} \in \mathcal{F}$*счетное семейство, тогда* $\cup\mathcal{A} \in \mathcal{F}$.

Теорема 3 (Теорема о проекции)**.** *Подмножество* $S \subseteq \mathbb{N}$ *счетно тогда и только тогда, когда оно является проекцией разрешимого подмножества декартового произведения* $\mathbb{N} \times \mathbb{N}$ *. Т.е.* $S = \{x \in \mathbb{N} | \exists y \in \mathbb{N}. \langle x, y\rangle \in \mathbb{N} \times \mathbb{N}\}$.

Следующее подмножество занимает исключительную роль в СТВ, а также хорошо известно в синтетической теории доменов. Мы покажем, что в СТВ счетные множества являются *полуразрешимыми*, предоставив такое множество $\Sigma \subseteq \Omega$ полуразрешимых истинных значений, что $\mathcal{E} = \Sigma^{\mathbb{N}}$.

Определение 19 (Множество полуразрешимых истинностных значений)**.**

$$\Sigma = \{p \in \Sigma | \exists f \in \mathbf{2}^{\mathbb{N}}.(p \iff (\exists n \in \mathbb{N}.f(n)))\}.$$

Σ также является *доминирующим* (см. [12]):

$$\forall p \in \Sigma.\forall q \in \Omega.((p \Rightarrow (q \in \Sigma)) \Longrightarrow (p \wedge q) \in \Sigma.$$

Приведем несколько утверждений, раскрывающих значение Σ.

Предложение 3. *Подмножество $\mathbb{N}$ счетно тогда и только тогда, когда оно полуразрешимо.*

Предложение 4. *Σ – это наименьшее подмножество Ω, содержащее $\top$ и замкнутое сверху.*

То, как эти множества соотносятся между собой, хорошо показывает следующая теорема (для доказательства см. [4]).

Теорема 4. *Ни одно из следующих включений $\mathit{2} \subseteq \Sigma \subseteq \Omega_{\neg\neg} \subseteq \Omega$ не является равенством.*

В классической логике все несколько проще: $\mathit{2} = \Omega$ со всеми вытекающими из этого равенства последствиями.

Рассмотрим широко известный в классической теории вычислений принцип Маркова.

Предложение 5. *Следующие утверждения эквивалентны:*

1. *Принцип Маркова: для каждого $a : \mathbb{N} \to \mathbf{2}, \neg(\forall n \in \mathbb{N}.a_n = 0) \Longrightarrow \exists n \in \mathbb{N}.a_n = 1$.*
2. *Полуразрешимые истинностные значения являются классическими $\Sigma \subseteq \Omega_{\neg\neg}$.*
3. *Полуразрешимые подмножества являются классическими.*
4. *Полуразрешимые подмножества $\mathbb{N}$ являются классическими.*

Хотя его выполнение является интуитивно бесспорным, доказать это в рамках конструктивной теории невозможно.

Аксиома 4 (Принцип Маркова)**.** *Двоичная последовательность, не являющаяся нулем, содержит единицу.*

С помощью этой аксиомы можно доказать следующую теорему, приводимую практически в каждой книге по теории вычислимости (по крайней мере для частного случая $A = \mathbb{N}$).

Теорема 5 (Поста)**.** *Подмножество множества A разрешимо тогда и только тогда, когда дополнение этого подмножества полуразрешимо.*

11. Основы СТВ

В этом параграфе будет дана последняя аксиома СТВ и несколько базовых теорем теории вычислений (которые удалось доказать в СТВ).

Определение 20. *Частичная* функция $f : A \rightharpoonup B$ – это функция $f : A' \to B$, определенная на подмножестве $A' \subseteq A$, называемом *носителем* f. Каждая частичная функция f соответствует (тотальной) функции $g : A \to \tilde{B}$, где $\tilde{B}$ – это множество частичных значений:

$$\tilde{B} = \{\mathcal{P}(B) | \forall x, y \in B.(x \in s \wedge y \in s \Longrightarrow x = y)\},$$

f и g соотносятся следующим образом: $g(x) = \{f(x) \in B | x \in A'\}$. Одноэлементное множество $\{y\}$ представляет собой полностью определенный элемент $y \in B$, который называется *совершенным* значением. Утверждение $\exists y \in B.(s = \{y\})$, означающее «частичное значение s совершенно», будем сокращать как $s\downarrow$.

Предложение 6. *Частичная функция $\mathbb{N} \to \tilde{\mathbb{N}}$ счетна (имеет счетный граф) тогда и только тогда, когда $f(n)\downarrow$ полуразрешимо для каждого $n \in \mathbb{N}$.*

Рассмотрим те частичные значения, чья совершенность полуразрешима.

Определение 21. Подъемом $A_\perp$ называется множество Σ-частичных значений

$$A_\perp = \{s \in \tilde{A} | s\downarrow \in \Sigma\},$$

Σ-частичная функция – это частичная функция $f : A \to B_\perp$.

Σ-частичные функции $\mathbb{N} \to \mathbb{N}_\perp$ являются синтетическими аналогами частично вычислимых функций. Классическая теорема теории вычислимости утверждает, что вычислимо-счетные множества в точности являются носителями частично вычислимых функций. Приведем аналогичное утверждение:

Предложение 7.
1. *Частиная функция является Σ-частичной тогда и только тогда, когда ее носитель полуразрешим.*
2. *Подмножество полуразрешимо тогда и только тогда, когда оно является носителем Σ-частичной функции.*

Представим еще одну хорошо известную теорему из классической теории.

Теорема 6 (Теорема об однозначности)**.** *Каждое полуразрешимое отношение R на $\mathbb{N} \times \mathbb{N}$ имеет Σ-частичную функцию выбора $s : A \to \tilde{B}$, такую, что для всех $x \in A$*

$$(\exists y \in B.R(x, y)) \Longrightarrow s(x)\downarrow \wedge R(x, s(x)).$$

В классической теории вычислений есть хорошо известные «теоремы счетности», первая из них утверждает, что «существует вычислимое перечисление вычислимо перечисляемых множеств», а вторая постулирует то же самое, но для частично вычислимых функций. В СТВ этим теоремам соответствуют следующая аксиома и утверждение 8. До сих пор все, что мы рассматривали, вполне может существовать в классической логике (при соответствующем переходе к классической теории множеств), хотя и не представляло бы тогда никакого интереса ($\mathbf{2} = \Sigma = \Omega$). Следующая аксиома в этом смысле является переломной – следствия из нее выходят за пределы классической логики.

Аксиома 5 (Счетности)**.** *Множество счетных подмножеств* $\mathbb{N}$ *счетно.*

Следующее утверждение является аналогом важной классической теоремы о вычислимости:

Предложение 8. $\mathbb{N} \to \mathbb{N}$ *счетно.*

Следующая теорема, которая является следствием аксиомы счетности, раскрывает суть возникающего в классической логике противоречия.

Теорема 7. *Ни одно из следующих включений не является равенством:*

$$\mathit{2} \subseteq \Sigma \subseteq \Omega_{\neg\neg} \subseteq \Omega.$$

Таким образом, мы получаем «невозможное» неравенство $\mathbf{2} \neq \Omega$. И наконец $\mathbf{2} \neq \Sigma$ означает, что семейства разрешимых и полуразрешимых подмножеств $\mathbb{N}$ не совпадают.

Предложение 9 (Принцип Фоа (Phoa))**.** *Для каждой* $f : \Sigma \to \Sigma$ *выполняются следующие два равенства:*

$$f(x) = (f(\bot) \vee x) \wedge f(\top) f(x) = f(\bot) \vee (x \wedge f(\top)).$$

12. Фокальные множества

После подъема множество приобретает «неопределенный» элемент $\bot_A$. Но иногда множество уже содержит такой «неопределенный» элемент. Например, он может быть получен путем присоединения $\top$ к множеству и затем отображением получившегося множества на исходное, не трогая элементы последнего. Таким образом, мы приходим к следующему определению.

Определение 22 (Фокальное множество)**.** *Фокальным множеством* называется множество A, взятое вместе с отображением (*фокусным*) $\epsilon : A_\bot \to A$, при котором $\epsilon(\{x\}) = x$ для всех $x \in A$. Элемент $\epsilon(\bot_A)$ называется *точкой фокуса.*

Говорят, что множество A *связно*, если оно не может быть разложено на несвязное объединение $A_1 + A_2$ нетривиальным способом. Другими словами, в связном множестве любое отображение $A \to \mathbf{2}$ является константой.
Основываясь на этом определении, в качестве заключения приведем две теоремы СТВ, являющиеся **более общими** аналогами теорем классической теории вычислений.

Теорема 8 (Райса). *Фокальное множество связно.*

Классическая теорема Райса утверждает, что не существует нетривиальных разрешимых подмножеств $\mathcal{E}$. Это сразу же следует из приведенной выше теоремы, т.к. $\mathcal{E}$ - фокальное множество.

Определение 23 (Многозначная функция). *Многозначной функцией* $f : A \rightrightarrows B$ называется функция $f : A \to \mathcal{P}(B)$, такая, что $f(x)$ не вырождено для каждого $x \in A$.

Стационарной точкой многозначной функции $f : A \rightrightarrows A$ называется такая точка $x \in A$, что $x \in f(x)$.

В завершение приведем обобщенную формулировку теоремы о рекурсии:

Теорема 9 (Теорема о рекурсии). *Каждая многозначная функция на счетном фокальном множестве имеет стационарную точку.*

Из теоремы 9 вытекает следующая классическая теорема.

Следствие 9.1 (Классическая теорема о рекурсии). *Для каждого* $f : \mathbb{N} \to \mathbb{N}$ *существует* $n \in \mathbb{N}$ *такое, что* $\varphi_{f(n)} = \varphi_n$.

13. Заключение

На данном этапе знакомство с синтетической теорией вычислений заканчивается. За рамками статьи остались описания пересечения СТВ с топологией, в частности теоремы Райса-Шапиро и Шефердсона, описывающие топологии на $\Sigma^{\mathbb{N}}$ и $\mathbb{N} \to \mathbb{N}_\perp$ соответственно. Фактически исследование рекурсивных топологий и рекурсивного анализа в рамках СТВ – это одно из направлений, напрашивающихся на разработку. Второе направление связано с изменением самого понятия вычисления и построением топосов, структура которых соответствовала бы данному понятию.

Небольшие достижения все же есть – формулировки и некоторые классические теоремы теории вычислимости выглядят в СТВ более элегантно. Доказаны аналоги основных теорем теории вычислимости (в некоторых случаях более общие), такие, как теорема Райса, теорема о рекурсии, теорема Поста, теорема об однозначности, теорема Райса-Шапиро и другие. По мнению автора, СТВ еще не успела вырасти до актуальных проблем теории вычислимости, что, несомненно, не способствует привлечению к ней внимания со стороны «классических» специалистов. Тем не менее автор уверен, что применение синтетического подхода поспособствует получению новых результатов.

Литература

1. Цаленко, М.С. Основы теории категорий / М.С. Цаленко. – М.: Наука, 1974.
2. Голдблатт, Р. Топосы. Категорный анализ логики / Р. Голдблатт. – М.: Мир, 1983.

3. Маклейн, С. Категории для работающего математика / С. Маклейн. – М.: ФИЗМАТЛИТ, 2004.
4. Bauer, A. First steps in synthetic computability theory / A. Bauer // Electr. Notes Theor. Comput. Sci. – 2006. – V.155. – P.5-31.
5. Johnstone, P. Sketches of an Elefant. A Topos Theory Compendum / P. Johnstone. – Oxford: Clarendon Press, 2002.
6. Johnstone, J.P. Sketches of an Elefant. A Topos Theory Compendum / J.P. Johnstone, A. Simpson // Annals of Pure and Applied Logic. – 2000.
7. Richman, F. Church's thesis without tears / F. Richman // The Journal of Symbolic Logic. – 1983. – V.48. – P.797-803.
8. Hyland, M. The effective topos / M. Hyland. – The L.E.J. Brouwer centerary symposium, 1982. – P.165-216.
9. Kock, A. Synthetic Differential Geometry / A. Kock. – Cambridge University Press, 2006.
10. Lavendhomme, R. Basic concepts of Synthetic Differential Geometry / R. Lavendhomme. – Kluwer Academic Publishers, 1996.
11. Phoa, W. An introduction to fibrations, topos theory, the effective topos and modest sets: Tech. rep. / W. Phoa. – The University of Edinburgh, 1992.
12. Rosolini, G. Continuity and effectiveness in topoi: Ph.D. thesis. – University of Oxford, 1986.
13. Rosolini, G. Domains in H. / G. Rosolini // Theoretical Computer Science, 2003. – V.2, N.264. – P.171-193.