Измерение сложности функций

В.К.Белошапка

18.11.2024

Аннотация

Обсуждается индуктивная схема измерения сложности. Рассмотрены примеры реализации данной схемы в контексте теории функций. Введено понятие суммы и произведения схем, схемы, подчиненной отображению. Получен ряд результатов, поставлены вопросы.

[1]

Рассмотрим следующую схему оценки сложности. Пусть нас интересует некоторая совокупность $\mathcal{U}$ математических объектов (универсальная совокупность). В этой совокупности выделено подмножество $\mathcal{B}$ "простых" (базовых, элементарных) объектов. Также зафиксирован список явно заданных правил $\mathcal{R}$, порождающих новые (более сложные) объекты. Причем подразумевается, что правила можно применять рекурсивно, т.е. применять пошаговые процедуры и строить новые объекты из уже построенных.

Если теперь предъявлен некий объект z из $\mathcal{U}$, то возникает два вопроса. Можно ли получить данный объект из элементарных за конечное число применений правил порождения? В случае положительного ответа мы получаем процедуру формирования данного объекта из некоторого набора базовых объектов (*схема композиции*). Зафиксируем некоторый способ характеризовать сложность полученной схемы композиции, т.е. некоторую неотрицательную целочисленную функцию (например, это может

[1]Механико-математический факультет Московского университета им. М.В.Ломоносова, Воробьевы горы, 119991 Москва, Россия, vkb@strogino.ru
Московский центр фундаментальной и прикладной математики МГУ им. М.В.Ломоносова

глубина самой длинной цепочки, использованной для формирования z (глубина рекурсии)). Тогда мы можем определить минимум этой функции по всем представлениям объекта z в виде такой композиции. Назовем эту величину "сложностью" z и обозначим $N(z)$. А в случае, если объект не обладает таким представлением, то сложность объекта полагаем равной бесконечности, т.е. $N(z) \in \{0, 1, 2, \dots, \infty\}$. Таким образом, возникает последовательность вложенных подмножеств $\mathcal{B} = Cl^0 \subset Cl^1 \subset \dots \subset \mathcal{U}$, где $Cl^n = \{z \in \mathcal{U} : N(z) \leq n\}$, т.е. Cl^n состоит из объектов сложности не выше чем n.

Свобода в выборе способа измерения сложности композиции весьма велика. Почти во всех примерах используется следующий способ. Припишем всем операциям из $\mathcal{R}$ целые неотрицательными веса (набор взвешенных операций). Тогда сложность композиции определяем так. Для каждой линейной цепочки последовательных подстановок, идущей от базового объекта к объекту z, вычисляем сумму весов. Т.е. если бы все веса были равны единице, то получаем просто глубину рекурсии. А если не все из весов равны единице, то получаем "взвешенную" глубину. Более того, в основном, будет использован следующий вариант: части операций назначаем вес единица, а остальным – ноль. Изредка мы выходим за рамки этого способа, что всегда явно оговаривается.

Определение 1: Описанный выше набор $\mathcal{S} = (\mathcal{U}, \mathcal{B}, \mathcal{R})$ (подразумевается, что операциям присвоены веса) будем называть *схемой оценки сложности*, а возникающую при этом последовательность Cl^n – *иерархией классов сложности.*

Каждая схема позволяет определить на всей совокупности объектов *функцию сложности* объекта $N(z)$, которая принимает значения в множестве $\{0, 1, \dots, \infty\}$.

Как видно из определения, каждый последующий класс строится однократным применением операции веса один к объектам из предыдущего класса. Т.е. классы порождаются индуктивно, и в этом смысле описанная схема является индуктивной. Представленная конструкция является весьма общей, хотя, конечно, не единственной. Эта конструкция является общематематической, т.е. она используется и в дискретной математике, и в геометрии, и в алгебре [1], [2], [3]. Но здесь нас, прежде всего, интересует ее реализация для совокупностей, состоящих из функций.

Схема 1. Универсальная совокупность $\mathcal{U}$ – это совокупность полиномов от одного переменного x с комплексными коэффициентами. Базовая совокупность объектов сложности ноль $\mathcal{B}$ – это постоянные. Единственное правило порождения (веса один): $\mathcal{R} = (p(x) \to a + x\,p(x))$, где a – произвольная постоянная.

Ясно, что в этом примере сложность полинома – это его степень. Отметим также, что в этом примере критерием принадлежности полинома $p(x)$ классу Cl^n является дифференциальное соотношение $p^{(n+1)}(x) = 0$. Все объекты имеют конечную сложность.

Схема 2.a. Совокупность $\mathcal{U}$ – это совокупность полиномов двух переменных (x, y). Объекты сложности ноль $\mathcal{B}$ – это константы. Правило порождения (вес – единица):

$$\mathcal{R} = \{(p(x,y), q(x,y)) \to a + x\,p(x,y) + y\,q(x,y)\},$$

где a – произвольная постоянная. В этом примере сложность полинома – это его степень по совокупности переменных. Все объекты имеют конечную сложность.

Не меняя $\mathcal{U}$ и $\mathcal{B}$, тот же самый результат можно получить иначе (*схема 2.b.*). В качестве $\mathcal{R}$ возьмем две операции веса один:

$$(p(x,y) \to x\,p(x,y)) \text{ и } (q(x,y) \to y\,q(x,y))$$

и третью веса ноль

$$(p(x,y), q(x,y)) \to p(x,y) + q(x,y).$$

Схема 2.c. Совокупность $\mathcal{U}$ – это совокупность полиномов двух переменных (x, y). Объект сложности ноль $\mathcal{B}$ – это полиномы, зависящие только от одного переменного. Два правила порождения $\mathcal{R}$ (веса единица):

$$R_1 = (p(x,y) \to q(x,y), \text{ если } \quad q'_x(x,y) = p(x,y)),$$
$$R_2 = (p(x,y) \to r(x,y), \text{ если } \quad r'_y(x,y) = p(x,y)).$$

Т.е. операция – это операция взятия первообразной по соответствующему переменному. При этом функцию определения сложности композиции определяем так: это максимум из двух чисел – количества применений первой операции и количества применений второй операции. В этом примере сложность полинома – это максимум его степеней по x и по y. Критерием принадлежности полинома $p(x,y)$ классу Cl^n являются два дифференциальных соотношения

$$\frac{\partial^{n+1}}{\partial x^{n+1}}\, p = 0, \qquad \frac{\partial^{n+1}}{\partial y^{n+1}}\, p = 0.$$

Пусть на одной универсальной совокупности имеются две схемы оценки сложности $\mathcal{S}_1$ и $\mathcal{S}_2$, которые могут отличаться как базовыми наборами, так и правилами порождения. Введем две естественные операции.

Определение 2: (a) *суммой* этих схем (обозначение $\mathcal{S}_1 \oplus \mathcal{S}_2$) назовем такую иерархию, которая задается условием

$$Cl^n = \{z \in \mathcal{U} : N(z) = \min(N_1(z), N_2(z)) \leq n\} = Cl_1^n \oplus Cl_2^n.$$

(b) *произведением* этих схем (обозначение $\mathcal{S}_1 \cdot \mathcal{S}_2$) назовем такую иерархию, которая задается условием

$$Cl^n = \{z \in \mathcal{U} : N(z) = \max(N_1(z), N_2(z)) \leq n\} = Cl_1^n \cdot Cl_2^n.$$

Комментарий к определению. Будем порождать объекты, пользуясь операциями из обеих схем. А старые схемы считаем вложенными в общую. При этом при подсчете $N_1(z)$ полагаем веса операций из $\mathcal{R}_2$ равными нулю, а при подсчете $N_2(z)$ – наоборот. После чего вычисляем $N(z)$ двумя разными для суммы и произведения способами.

Обе операции коммутативны и ассоциативны, а также связаны соотношением дистрибутивности. Для каждой этих операций существует нейтральный элемент. $\mathbf{0}$ – для суммы и $\mathbf{1}$ – для произведения. $\mathbf{0}$ – это схема, в которой $\mathcal{B} = \emptyset$ и все объекты имеют бесконечную сложность. А $\mathbf{1}$ – схема, где $\mathcal{U} = \mathcal{B}$ и все объекты имеют сложность ноль.

$$\forall \mathcal{S} \quad \mathcal{S} \oplus \mathbf{0} = \mathcal{S}, \quad \mathcal{S} \cdot \mathbf{1} = \mathcal{S}.$$

Схема 3. В примере 1 изменим совокупность $\mathcal{U}$. Пусть $\mathcal{U}$ – это все целые функции переменного x. А правило порождения оставим прежним. Картина меняется следующим образом. Пространство функций конечной сложности – это подпространство полиномов, которое является собственным подпространством в пространстве всех целых функций. Все неполиномиальные целые функции имеют сложность равную бесконечности.

Схема 4. Пусть $\mathcal{U}$ – это пространство комплекснозначных вещественно-аналитических функций, определенных на всей комплексной плоскости, т.е. $f = f(x, \bar{x})$, а $\mathcal{B}$ – это подпространство целых функций переменного x. Операция (веса единица):

$$(f(x,\bar{x}), g(x,\bar{x})) \to f(x,\bar{x}) + \bar{x}\, g(x,\bar{x}).$$

Ясно, что в результате конечную сложность имеют только полиномы от $\bar{x}$ (полианалитические функции), чьи коэффициенты – это целые функции, причем сложность – это степень по $\bar{x}$.

Схема 5. $\mathcal{U}$ – это аналитические функции от (x, y), $\mathcal{B}$ – это аналитические функции, зависящие лишь от одного переменного (либо x, либо y). Два правила порождения $\mathcal{R} = (R_1, R_2)$, которые определим так. Пусть $p(x, y)$ и $q(x, y)$ – голоморфные элементы, представляющие аналитические функции P и Q, а $s(t)$ – голоморфный элемент, представляющий аналитическую функцию одного переменного S, тогда

$$R_1 = (\ (p(x,y), q(x,y)) \to p(x,y) + q(x,y)\ )\,,\ \text{вес – единица},$$
$$R_2 = (\ p(x,y) \to s(p(x,y))\ )\,,\ \text{вес – ноль}.$$

Это пример, изучению которого посвящена серия статей [8], [9], [10]. При этом возникает иерархия классов Cl^n и для каждой аналитической функции $z(x, y)$ определена *аналитическая сложность* $N(z)$. Каждый класс имеет определяющую его систему дифференциально-полиномиальных уравнений. Причем если Cl^0 и Cl^1 имеют простые определяющие соотношения, то, начиная с Cl^2, сложность соответствующих дифференциальных полиномов стремительно растет [11]. Отметим, что несложно написать общий вид функции из Cl^n. Для этого требуется иметь $2^{n+1} - 1$ аналитическую функцию одного переменного и составить из них общую формулу композиции глубины n.

Схема 6. Схему 5 можно модифицировать следующим образом. В R_1 сложение $u + v$ заменить на произвольную фиксированную аналитическую функцию двух переменных $\varphi(u,v)$. Возникает модифицированная последовательность классов Cl^n_φ и модифицированная аналитическая сложность $N_\varphi(z)$.

Универсальная совокупность, как мы видели, может содержать объекты бесконечной сложности, а может и не содержать. В частности, для схем 3, 4, 5 и 6, в отличие от схем 1 и 2, как нетрудно убедиться, функция "общего положения" имеет бесконечную сложность. При этом все рассмотренные иерархии являются бесконечно растущими. Приведем примеры, для которых иерархия сводится к конечному числу классов.

Схема 7. В определении схемы 5 изменим универсальную совокупность (сужение схемы). Пусть $\mathcal{U}$ – это аналитические функции $z(x,y)$, являющиеся решениями уравнения Лапласа $z''_{xx}+z''_{yy}=0$ (или, как вариант, волнового уравнения $z''_{xx}-z''_{yy}=0$). А правила порождения новых объектов оставим прежними (сложение и композиция с аналитическими функциями одного переменного). В силу того, что любое решение уравнения Лапласа можно записать в виде $z(x,y)=f(x+i\,y)+g(x-i\,y)$, иерархия классов стабилизируется, начиная со второго, т.е.

$$\mathcal{B}=Cl^0\subset Cl^1\subset Cl^2=Cl^3=\ldots=\mathcal{U}.$$

Решения уравнения Лапласа сложности ноль, т.е. $\mathcal{B}=Cl^0$, – это линейные функции одного переменного, гармонические функции общего положения попадают в Cl^2. Уместно задать вопрос, что представляют собой гармонические функции из Cl^1? Тривиальная компонента этого класса – это функции вида $f(x+i\,y)$ и $g(x-i\,y)$, а нетривиальная – это некоторое конечномерное семейство функций, выражающихся через эллиптические [12].

Глядя на эту ситуацию, нетрудно дать общее определение *сужения схемы.*

Схема 8. Пусть $\mathcal{U}$ – это непрерывные функции на квадрате $\{0\le x\le 1,\ 0\le y\le 1\}$, базовый набор $\mathcal{B}$ – это непрерывные функции одного переменного (x или y). Правила порождения – те же, что и в схеме 5, с заменой аналитических функций на непрерывные. По теореме Колмогорова [4] любая непрерывная на квадрате функция имеет представление вида

$$f(x,y)=c_1(a_1(x)+b_1(y))+c_2(a_2(x)+b_2(y))+ \tag{1}$$

$$c_3(a_3(x)+b_3(y))+c_4(a_4(x)+b_4(y))+c_5(a_5(x)+b_5(y)).$$

Утверждение 1. Если Cl^n – это классы сложности в схеме примера 8, то эта иерархия стабилизируется не позже четвертого члена, т.е. $Cl^{4+n}=Cl^4$, $n\geq 0$.
Доказательство: В этой схеме

$$N\left(c(a(x)+b(y))\right)\leq 1,$$
$$N\left(c_1(a_1(x)+b_1(y))+c_2(a_2(x)+b_2(y))\right)\leq 2,$$
$$N\left(c_1(a_1(x)+b_1(y))+\ldots+c_4(a_4(x)+b_4(y))\right)\leq 3,$$
$$N\left(c_1(a_1(x)+b_1(y))+\ldots+c_4(a_4(x)+b_4(y))+c_5(a_5(x)+b_5(y))\right)\leq 4.$$

Теперь утверждение следует из теоремы Колмогорова.

В связи с этим примером можно сформулировать два вопроса.

Вопрос 1. На каком шаге n стабилизируется данная иерархия?

Известно [5], что $Cl^1\neq\mathcal{U}$. Поэтому, если принять во внимание утверждение 1, вариантов ответа три: $n=2,3,4$. Доказано [6], что суммами вида (1) с четырьмя слагаемыми нельзя представить все непрерывные на квадрате функции.

Вопрос 2. Если имеется непрерывная на квадрате функция $z(x,y)$, то как проверить, попала эта функция в Cl^1 или нет?

Для трижды гладких функций критерием является нелинейное дифференциально-полиномиальное уравнение с частными производными третьего порядка [8]. Для дважды гладких этот критерий можно переписать, используя аппарат обобщенных функций (распределений). А для гладких и, тем более, непрерывных не ясна даже природа такого критерия.

Схема 9. Пусть $\mathbf{C}$ – это поле комплексных чисел, пусть $\mathbf{C}(x)$ – это поле рациональных функций одного переменного x. Т.е. расширение, порожденное присоединением алгебраически независимого элемента x. Пусть $\mathcal{U}$ – это алгебраическое замыкание поля $\mathbf{C}(x)$ (поле алгебраических функций от x). Это означает следующее: если $P(z)$ – полином от z с коэффициентами из $\mathbf{C}(x)$ и $P(f)=0$, то $f\in U$. Положим $\mathcal{B}=\mathbf{C}(x)$.

Список операций $\mathcal{R} = (R, R_1, R_2, R_3, R_4)$:

$$R = (a \to f, \text{ т.ч. } f^m = a), \quad \text{вес – единица},$$
$$R_j = (\ (a, b) \to a * b\ ), \quad \text{вес – ноль},$$
$$\text{где } * \text{ – любая из четырех арифметических операций.}$$

Т.е. R – это присоединение корня степени m, а (R_1, R_2, R_3, R_4) – это построение нового подполя. Возникающая при этом иерархия классов позволяет определить $N(z)$ – сложность алгебраической функции. Эта величина измеряет максимальную длину цепочки вложенных радикалов, необходимых для представления функции. Совокупность $\mathcal{K}$ функций конечной сложности – это функции, имеющие представление с помощью радикалов. В соответствии с теоремой Абеля [7] поле $\mathcal{K}$ – собственное подполе $\mathcal{U}$, т.е. существуют алгебраические функции бесконечной сложности. Простейшим примером такой функции является функция $z(x)$, заданная полиномом степени пять $z^5 + x\,z + 1 = 0$.

Схема 10. $\mathcal{U}$ – это поле алгебраических функций от (x, y). Поясним, что имеется в виду. Пусть $\mathbf{C}$ – это поле комплексных чисел, пусть $\mathbf{C}(x, y)$ – это чисто трансцендентное расширение $\mathbf{C}$ степени два, т.е. расширение, порожденное присоединением двух алгебраически независимых элементов x и y (поле рациональных функций от (x, y)). Пусть $\mathcal{U}$ – это алгебраическое замыкание поля $\mathbf{C}(x, y)$ (поле алгебраических функций от (x, y)). Это означает следующее: если $P(z)$ – полином от z с коэффициентами из $\mathbf{C}(x, y)$ и $P(f) = 0$, то $f \in \mathcal{U}$. Положим $\mathcal{B} = \mathbf{C}(x, y)$. В качестве операций $\mathcal{R}$ рассмотрим операцию построения расширения L поля K путем присоединения композиции элементов K с *каждой алгебраической функцией одного переменного* и порождения этими элементами нового поля. Итак, $\mathcal{R} = (R, R_1, R_2, R_3, R_4)$:

$$R = (\ (a_0, a_1, \ldots, a_m) \to f\ ) : a_0 + a_1\,f + \ldots + a_m\,f^m = 0 \quad \text{вес } 1,$$
$$R_j = ((a, b) \to a * b), \quad \text{вес } 0,$$
$$\text{где } * \text{ – одна из четырех арифметических операций.}$$

В результате мы получаем расширяющуюся последовательность подполей $\mathbf{C}(x, y)$

$$\mathbf{C}(x, y) = Cl^0 \subset Cl^1 \subset \ldots \subset \mathcal{U}$$

и можем рассмотреть поле $\mathcal{F} = \bigcup_{n=0}^{\infty} Cl^n$, образованное всеми элементами конечной сложности. С этим полем связан вопрос, ответ на который автору не известен.

Вопрос 3. Является ли это подполе собственным или же $\mathcal{F} = \mathcal{U}$? Т.е. исчерпывает ли эта иерархия все алгебраические функции от двух переменных или нет?

Отметим, что поле $\mathcal{F}$ замкнуто относительно частных дифференцирований (по x и по y), т.е. является дифференциальным полем.

Алгебраические функции (универсальная совокупность примера 10) – это подмножество множества аналитических функций (универсальная совокупность примера 5). Аналогично базовая совокупность примера 10 – это подмножество базовой совокупности примера 5 (функции одного переменного). Учитывая, что порождающие правила примера 5, примененные к алгебраическим функциям, не выводят нас за рамки алгебраических функций, мы видим, что схема 5 индуцирует на совокупности схемы 10 новую схему (схема 5'), которая является сужением схемы 5.

Ясно, что обе сложности $N_1(z)$ – аналитическая (из примера 5') и $N_2(z)$ – алгебраическая (из примера 10), а также соответствующие классы сложности (обозначим их Cl_1^n и Cl_2^n) различаются весьма существенно. Отметим здесь одно из различий. Все Cl_1^n – это дифференциально-алгебраические множества (задаются системами дифференциально-полиномиальных соотношений с рациональными коэффициентами).

Утверждение 2. Ни один из классов алгебраической сложности Cl_2^n не является дифференциально-алгебраическим множеством. Более того, не существует нетривиального дифференциального полинома (с комплексными коэффициентами), который бы обращался в ноль на всех функциях класса.
Доказательство: Все классы (включая нулевой) содержат $C[x, y]$ – полиномы от (x, y). А если дифференциальный полином обращается в ноль на каждом полиноме из $C[x, y]$, то он тождественно равен нулю.

К этому можно добавить, что все Cl_2^n – это поля, в отличие от Cl_1^n, которые, очевидно, не замкнуты относительно арифметических операций.

Наличие на одной совокупности двух схем позволяет нам рассмотреть их сумму и произведение.

Вопрос 4. Что собой представляют алгебраические функции, составляющие первый класс для произведения схем? Т.е. требуется явно описать $Cl_1^1 \cdot Cl_2^1$.

Критерий попадания в Cl_1^1 известен и прост. Не ясно, как контролировать попадание в Cl_2^1.

Вопрос 5. Что представляет собой критерий попадания в класс для схем 9 и 10? Т.е. как и для вопроса 2 (схема 8) не ясна математическая природа такого критерия и мера его конструктивности.

Схемы 1, 3 и 4 отличаются от других примеров тем, что в них имеется оператор T, действующий на $\mathcal{U}$ т.ч. $Cl^n = \{z \in \mathcal{U} : T^{(n+1)}(z) = 0\}$ (подразумевается, что $T^{(n)}$ – это n-я итерация T). Обобщая эти примеры, дадим новое определение. Причем, несмотря на то, что в данных примерах $\mathcal{U}$ – это линейное пространство, а T – линейный оператор из $\mathcal{U}$ в $\mathcal{U}$, мы не будем этого заранее предполагать.

Определение 3. Говорим, что схема оценки сложности $\mathcal{S} = (\mathcal{U}, \mathcal{B}, \mathcal{R})$ *подчинена* отображению $T : \mathcal{U} \to \mathcal{U}$, если $Cl^n = \{z \in \mathcal{U} : T^{(n+1)}(z) \in \mathcal{B}\}$.

Ясно, что если мы имеем дело со схемой оценки сложности, подчиненной отображению T универсальной совокупности в себя, то классы сложности – это последовательные прообразы базовой совокупности по отношению к итерациям T, т.е. $Cl^n = (T^{(n+1)})^{-1}(\mathcal{B})$. Причем правило порождения $\mathcal{R}$ однозначно определяется через T, а именно, $\mathcal{R} = (z \to \forall w \in T^{-1}(z))$. Таким образом, отображение T^{-1} – это отображение усложнения, а T – упрощения.

В контексте схемы, подчиненной отображению, можно предложить следующее достаточное условие бесконечной сложности объекта, которое сразу следует из определения.

Утверждение 3. (a) Пусть имеется схема $\mathcal{S}$, подчиненная отображению T, и $z \notin \mathcal{B}$, причем $T(z) = z$ (неподвижная точка), тогда $N(z) = \infty$.

(b) Если в этой схеме $\mathcal{U}$ – линейное пространство, $T:\mathcal{U}\to\mathcal{U}$ – линейный оператор, а $T\,z=\lambda\,z$ – собственный вектор, т.ч. $\lambda\neq 0$, то $N(z)=\infty$.

Схема 11. Пусть $\mathcal{U}$ – это целые функции переменных (x,y), а $\mathcal{B}$ – это тождественный ноль. Положим

$$T=\frac{\partial^2}{\partial\, x\,\partial\, y},\ \text{тогда}\quad T^{-1}=D_x^{-1}\circ D_y^{-1},$$

где D_x^{-1} и D_x^{-1} – операторы неопределенного интегрирования по x и y соответственно, включающие в себя выбор произвольной константы. Тогда получаем

$$Cl^1=T^{-1}(0)=\{z=a(x)+b(y)\},$$
$$Cl^2=(T^{(2)})^{-1}(0)=\{z=a(x)+b(y)+x\,B(y)+y\,A(x)\},\ldots$$

Пусть $Z_+=\{0,1,2,\ldots\}$. Если $f(x,y)=\sum c_{mn}x^my^n$ – целая функция, то носитель $\operatorname{supp} f$ – это подмножество Z_+^2 образованное парами (m,n), т.ч. $c_{mn}\neq 0$.

Утверждение 4. (a) Cl^n в схеме 11 – это все целые функции f т.ч. $\operatorname{supp} f$ содержится в объединении двух полос $\{0,1,\ldots,n-1\}\times Z_+$ и $Z_+\times\{0,1,\ldots,n-1\}$.
(b) Сложность $N(\exp(x+y))=\infty$.
Доказательство: (a) доказывается по индукции, (b) следует из того, что $T(\exp(x+y))=\exp(x+y)$.

Схема 12. Приведем пример схемы, подчиненной отображению T, где это отображение не является линейным. Пусть $\mathcal{U}$ – это мероморфные на $\mathbf{C}$ функции, не равные тождественному нулю, $\mathcal{B}$ – ненулевые константы. Положим

$$T(f(z))=f'(z)/f(z)\ \text{(логарифмическая производная)},$$
$$\text{тогда}\ \ T^{-1}(g(z))=\exp(D^{-1}(g(z))).$$

Если a – ненулевая постоянная, тогда получаем

$$Cl^1=T^{-1}(a)=\{z=a_1\,\exp(a\,x)\},\ a_1\neq 0$$
$$Cl^2=(T^{(2)})^{-1}(a)=\{z=a_2\,\exp\left(\frac{a_1}{a}\,\exp(a\,x)\right)\},a_2\neq 0.$$

Утверждение 5. В контексте схемы 12 имеем:
(a) Cl^n – это конечнопараметрическое семейство целых функций, чья размерность равна $(n+1)$.
(b) Любая функция, не являющаяся целой, имеет сложность равную бесконечности.
Доказательство: (a) доказывается по индукции, (b) очевиден.

В схеме 2 у нас было два порождающих правила и, соответственно, эта ситуация для своего описания в стиле данного выше определения требует не одного, а двух операторов ($\mathcal{U}$ и $\mathcal{B}$ сохраняем прежними). Положим

$$T_1 = \frac{\partial}{\partial x}, \qquad T_2 = \frac{\partial}{\partial y},$$

тогда

$$Cl^n = \{z \in \mathcal{U} : T_1^{(n+1)}(z) \in \mathcal{B},\ T_2^{(n+1)}(z) \in \mathcal{B}\}.$$

При этом говорим, что данная схема подчинена паре операторов (T_1, T_2).

Вернемся к схеме 5. Как хорошо известно [8], критерием попадания аналитической функции $z(x,y)$ в $Cl^1 \setminus Cl^0$ является соотношение

$$T(z) = \left(\log\left(\frac{z'_x}{z'_y}\right)\right)''_{xy} = 0. \tag{2}$$

При этом решения данного уравнения имеют вид $z(x,y) = c(a(x) + b(y))$, где (a,b,c) – непостоянные аналитические функции одного переменного. Воспользуемся оператором (2), чтобы определить новую схему для той же универсальной совокупности.

Схема 13. Пусть $\mathcal{U}$ – как в примере 5, $\mathcal{B} = \{z(x,y) = c(a(x) + b(y))\}$, и отображение T, задающее классы сложности, задано соотношением (2).

Чтобы построить оператор T^{-1} нужно решить уравнение

$$T(z) = \left(\log\left(\frac{z'_x}{z'_y}\right)\right)''_{xy} = \varphi(x,y) \tag{3}$$

для произвольной аналитической функции $\varphi(x,y)$. Поскольку этот оператор – это композиция трех отображений $T = L\circ\log\circ H$, где

$$L : w \to \frac{\partial^2 w}{\partial x\,\partial y},\quad \log : w \to \log(w),\quad H := w \to \frac{w'_x}{w'_y},$$

то $T^{-1} = H^{-1}\circ\exp\circ L^{-1}$. Оператор $L^{-1} = D_x^{-1}\circ D_y^{-1} + \alpha(x) + \beta(y)$. Рассмотрим уравнение $H(z(x,y)) = \varphi(x,y)$, или

$$z'_x - \varphi(x,y)\,z'_y = 0. \tag{4}$$

Это линейное дифференциальное уравнение. Соответствующее характеристическое уравнение имеет вид

$$dx = -\frac{dy}{\varphi(x,y)}\quad \text{или}\quad \frac{dy}{dx} = -\varphi(x,y) \tag{5}$$

Решая это обыкновенное дифференциальное уравнение 1-го порядка, получаем общее решение (первый интеграл) $\Theta(x,y) = C$, где C – произвольная постоянная. Таким образом, общее решение уравнения (4) имеет вид $z(x,y) = H^{-1}(\varphi) = \gamma(\Theta(x,y))$, где $\gamma(t)$ – произвольная аналитическая функция одного переменного. Итого, получаем:

Теорема 6. (a) $T^{-1} = H^{-1}\circ\exp\circ L^{-1}$, где

$$L^{-1} = D_x^{-1}\circ D_y^{-1} + \alpha(x) + \beta(y),\quad H^{-1}(\varphi(x,y)) = \gamma(\Theta(x,y)),$$

и где (α,β,γ) – произвольные функции одного переменного, $\Theta(x,y)$ – первый интеграл уравнения (5).
(b) Класс Cl^n для схемы 13 – это семейство аналитических функций двух переменных, аналитически зависящих от $3(n+1)$ функций одного переменного.

Пусть на одной и той же универсальной совокупности $\mathcal{U}$ имеется две схемы оценки сложности $\mathcal{S}_1$ и $\mathcal{S}_2$. Им соответствуют две иерархии классов $\{Cl_1^n\}, \{Cl_2^n\}$ и две функции сложности $(N_1(z), N_2(z))$.

Определение 4: (a.1) Говорим, что $\mathcal{S}_1$ и $\mathcal{S}_2$ – слабо эквивалентны (пишем $\mathcal{S}_1 \sim \mathcal{S}_2$), если $N_1(z) < \infty$ тогда и только тогда, когда $N_2(z) < \infty$.
(a.2) Говорим, что $\mathcal{S}_1$ и $\mathcal{S}_2$ – сильно эквивалентны (пишем $\mathcal{S}_1 \approx \mathcal{S}_2$), если

для всех z выполнено $N_1(z) = N_2(z)$.
(b.1) Говорим, что $\mathcal{S}_2$ слабо мажорирует $\mathcal{S}_1$ (пишем $\mathcal{S}_1 \preceq \mathcal{S}_2$), если из $N_2(z) < \infty$ следует, что $N_1(z) < \infty$.
(b.2) Говорим, что $\mathcal{S}_2$ сильно мажорирует $\mathcal{S}_1$ (пишем $\mathcal{S}_1 \leq \mathcal{S}_2$), если для всех z выполнено $N_1(z) \leq N_2(z)$.

Нетрудно проверить справедливость следующих утверждений.

Утверждение 7. Это определение корректно в том смысле, что оно:
(a) удовлетворяет требованиям к формальному отношению эквивалентности и, тем самым, все схемы оценки сложности на данном универсальном множестве распадаются на классы эквивалентности (пишем $[\mathcal{S}]_w$ для слабой эквивалентности и $[\mathcal{S}]_s$ для сильной),
(b) отношение мажорирования удовлетворяет требованиям к формальному отношению частичного порядка,
(c) введенное отношение порядка корректно переносится со схем на классы эквивалентных схем,
(d) операции суммы и произведения схем, введенные в определении 2, корректно переносятся на классы эквивалентных схем.

Отметим, что $[\mathbf{0}]_w = [\mathbf{0}]_s = \mathbf{0}$, $[\mathbf{1}]_w$ – это любая схема, где все сложности конечны, а $[\mathbf{1}]_s$ – это любая схема, где все сложности равны нулю. Классы $[\mathbf{0}]_w = [\mathbf{0}]_s$, $[\mathbf{1}]_w$ и $[\mathbf{1}]_s$ остаются нейтральными элементами для сложения и умножения.

В связи с пунктом (d) утверждения 8 уместно дать следующее определение:

Определение 5. (a) Говорим, что схема $\mathcal{S}$ – разложима, если $\mathcal{S} = \mathcal{S}_1 \oplus \mathcal{S}_2$, где $\mathcal{S}_1 \neq \mathbf{0}$ и $\mathcal{S}_2 \neq \mathbf{0}$.
(b) Говорим, что класс схем $\mathcal{S}$ – приводим, если $\mathcal{S} = \mathcal{S}_1 \cdot \mathcal{S}_2$, где $\mathcal{S}_1 \neq \mathbf{1}$ и $\mathcal{S}_2 \neq \mathbf{1}$.

Ясно, эти определения переносятся на классы эквивалентных схем.

При разложении нуля возникает пара схем, взаимно обратных по сложению, а при разложении единицы – по умножению. Здесь есть простор для новых определений и конструкций. Можно говорить о морфизмах и изоморфизмах схем, о подсхемах, о тензорных произведениях. Можно также рассматривать другие виды эквивалентности схем и т.д. Но все это выходит за рамки данной статьи.

Вернемся к исходному определению 1. С каждой схемой связано две задачи. Задача построения произвольного объекта из Cl^n и задача проверки конкретного объекта на принадлежность Cl^n (задача идентификации). Описание схемы, в соответствии с определением, дает решение первой задачи. Схема – это, по существу, рекурсивное описание алгоритма построения объекта. Со второй задачей все совершенно иначе. Ее решение подразумевает построение конструктивного критерия принадлежности классу Cl^n. При этом как само существование такого критерия, так и мера его конструктивности – это вопросы, ответы на которые зависят от конкретной схемы (см. схемы 8, 9 и 10).

Рассмотрим схему 5. Общий вид функции сложности не выше чем n строится очевидным образом. Для построения требуется набор из $2^{n+1}-1$ функций одного переменного. В частности, для $n = 2$ это выглядит так:

$$z(x, y) = s(c(a(x) + b(y)) + r(p(x) + q(y))).$$

Критерий принадлежности функции z классу Cl^n – это условие обращения в ноль всех элементов некоторого дифференциального идеала в дифференциальном кольце $\mathbf{Q}[z, D_x, D_y]$. Этот идеал имеет конечный набор образующих, которые вычисляются конструктивно. Но, как было сказано выше, это вычисление является очень сложным [12]. Используя вычислительную асимметрию между первой и второй задачами, можно предложить очень надежный способ шифрования сигнала [13].

Однако если речь идет о схеме, подчиненной отображению T (определение 3), то ситуация меняется. Вторая задача сразу получает решение. Критерий принадлежности объекта z классу Cl^n – это условие $T^{(n+1)}(z) \in \mathcal{B}$. Тогда как для решения первой задачи требуется построение последовательных прообразов по отношению к отображению T базовой совокупности $\mathcal{B}$ и далее. Эту асимметрию в пользу второй задачи демонстрирует схема 13. Для решения задачи идентификации функции $z(x, y)$ требуется вычисление $(n+1)$-й итерации несложного дифференциально-рационального выражения. Описание решения задачи построения общей функции сложности n выглядит сложнее (см. теорему 6), чем решение задачи идентификации.

Предположим, что для некоторой схемы $\mathcal{S}$ вопрос о существовании конструктивного критерия принадлежности классу решен положительно (как, например, для схемы 5). Пусть при этом мы уточнили, как мы будем понимать конструктивность, т.е. зафиксированы средства описания алгоритмов (язык $\mathcal{L}$). Подразумевается, что $\mathcal{L}$ позволяет алгоритмически описать операции порождения $\mathcal{R}$ из нашей схемы, а также критерии принадлежности классу. Тогда мы можем использовать подход Колмогорова [14] для того, чтобы определить асимметрию схемы $\mathcal{S}$. Отметим при этом, что колмогоровская сложность в рамки определения 1, по крайней мере непосредственно, не вписывается. Это другой подход к оценке сложности.

Фиксируем n. Пусть $K_1^n(\mathcal{S})$ и $K_2^n(\mathcal{S})$ – это минимальные длины записи алгоритма решений первой (построение общего объекта) и второй (идентификация) задач. Тогда в качестве меры асимметрии схемы $\mathcal{S}$ можно предложить отношение $K_2^n(\mathcal{S})/K_1^n(\mathcal{S})$. Отметим, что сильная асимметрия между первой и второй задачей, как в одну сторону, так и в другую, несет в себе возможность построения систем шифрования наподобие той, что была представлена в [13].

Список литературы

[1] Д.Э.Сэвидж, Сложность вычислений, "Факториал", Москва, 1998, 368 с.

[2] В.В.Прасолов, А.Б.Сосинский, Узлы, зацепления, косы и трехмерные многообразия, МЦНМО, 1997, 352 с.

[3] В.А.Васильев, Топология дополнений к дискриминантам, Фазис, Москва, 1997, 536 с.

[4] А. Н. Колмогоров, "О представлении непрерывных функций нескольких переменных в виде суперпозиций непрерывных функций одного переменного и сложения", Докл. АН СССР, 114:5 (1957), 953–956.

[5] В. И. Арнольд, "О представимости функций двух переменных в виде $\chi(\varphi(x) + \psi(y))$", УМН, 12:2(74) (1957), 119–121.

[6] R.Doss, On the representation of the continuous functions of the two variables by means of the addition and continuous functions of one variable, Colloq/Math. 1963, v.10, p. 249-259.

[7] В.В.Прасолов, Ю.П.Соловьев, Эллиптические и алгебраические функции, "Факториал", Москва, 1997, 288 с.

[8] Beloshapka V. K. Analytic complexity of functions of two variables //Russian Journal of Mathematical Physics. – 2007. – T. 14. – №. 3. – C. 243-249.

[9] Beloshapka V. K. Analytical complexity: Development of the topic //Russian Journal of Mathematical Physics. – 2012. – T. 19. – №. 4. – C. 428-439.

[10] Beloshapka V. K. Decomposition of Functions of Finite Analytical Complexity // Journal of Siberian Federal University. Mathematics and Physics 2018, 11(6), 680–685.

[11] В. К. Белошапка, "О сложности дифференциально-алгебраического описания классов аналитической сложности", Матем. заметки, 105:3 (2019), 323–331; Math. Notes, 105:3 (2019), 309–315.

[12] Beloshapka V. K. On Simple Solutions of Some Equations of Mathematical Physics //Russian Journal of Mathematical Physics. – 2020. – T. 27. – C. 309-325.

[13] V. K. Beloshapka, Analytical Complexity and Signal Coding,Russian Journal of Mathematical Physics, Vol. 30, No. 4, 2023, pp. 501–521.

[14] А. Н. Колмогоров, "Три подхода к определению понятия "количество информации"", Пробл. передачи информ., 1:1 (1965), 3–11.