ЛОГИЧЕСКИЕ МЕТОДЫ В ПРОГРАММИРОВАНИИ
(Вычислительные системы)
1990 год Выпуск 133

УДК 517.11:518.5

АКСИОМАТИЗАЦИЯ ВЫЧИСЛЕНИЙ С ОРАКУЛАМИ И КОНТИНУУМ-ГИПОТЕЗА

В.А. Ганов

Рассматривается новое изложение следующего известного факта о континуум-гипотезе: при подходящем выборе оракула можно построить машинно-оракульную модель анализа, в которой выполняется естественный вариант континуум-гипотезы. В [1] этот факт был доказан с использованием так называемых сильно фундированных оракулов. В данной работе сильная фундированность заменяется специальным условием разложимости оракула, введенным в [2]. Причем известен пример оракула, разложимого, но не являющегося сильно фундированным [3]. Кроме того, в [1] производится непосредственное построение указанной модели анализа, но интереснее было бы вывести континуум-гипотезу из подходящей системы аксиом, описывающей естественные требования к оракулу. Именно такой подход рассматривается в данной работе. В качестве искомой системы $A(F)$ берется система, описанная в [4], к которой добавлена аксиома о разложимости оракула F.

Для удобства чтения в §1 формулируются необходимые сведения общей теории вычислений с оракулами, доказательства которых легко воспроизводятся в $A(F)$. В §2 описывается система $A(F)$, в §3 излагается основной результат. Для некоторых утверждений приведены полные доказательства с иллюстративной целью, чтобы читатель видел, что соответствующие построения действительно формализуемы в $A(F)$.

§1. Вычисления с оракулом

Машина с оракулом - это обычная машина Тьюринга, снабженная специальным входом для общения с оракулом, и в программу которой введены специальные спрашивающие команды. Оракул - произвольная числовая функция F (вообще говоря, невычислимая и не всюду определенная), которая ставится на указанный вход машины. Вопросы - произвольные числа, которые вычисляются данной машиной, а ответы на них - соответствующие им значения оракула. Если машина, соединенная с оракулом F, вычислила некоторый вопрос x, а значение оракула $F(x)$ не определено, то и результат работы этой машины считается неопределенным, - говорят, что машина с оракулом F застряла на вопросе x.

Стандартным образом вводится гёделевская нумерация машин с оракулом. Запись $\{z\}^F(x)$ обозначает функцию от x, вычислимую на машине с гёделевским номером z и соединенную с оракулом F. Такую функцию будем называть F-вычислимой, а z - F-номером этой функции. Предполагается также, что зафиксирована гёделевская нумерация кортежей натуральных чисел, $\langle x_1, x_2, \ldots, x_n\rangle$ обозначает гёделевский номер кортежа $(x_1, x_2, \ldots, x_n)$. Гёделевский номер пары $\langle z, x\rangle$, составленный из номера машины z и ее аргумента x, называется инициальной машиной. Выражение $\langle z, x\rangle_F$ обозначает инициальную машину, соединенную с оракулом F. Пусть $B(F)$ - множество инициальных машин, которые останавливаются при работе с оракулом F; $\widetilde{B}(F)$ - множество инициальных машин, не застревающих с F; δF - область определения F; $B^*(F)$ - множество F-номеров всюду определенных одноместных F-вычислимых функций.

ОПРЕДЕЛЕНИЕ 1. Множество M называется F-разрешимым, если его характеристическая функция F-вычислима. Множество M

называется $\mathbf{F}$-перечислимым, если оно является областью определения $\mathbf{F}$-вычислимой функции, при этом $\mathbf{F}$-номер этой функции называется $\mathbf{F}$-индексом $\mathbf{M}$.

Аналогично определяются $\mathbf{F}$-разрешимые и $\mathbf{F}$-перечислимые предикаты.

ТЕОРЕМА 1. *Для любого оракула* $\mathbf{F}$: *а) класс* $\mathbf{F}$*-разрешимых множеств замкнут относительно операций объединения, пересечения, разности и декартова произведения; б) класс* $\mathbf{F}$*-разрешимых предикатов замкнут относительно логических операций конъюнкции, дизъюнкции, импликации и отрицания; в) класс* $\mathbf{F}$*-вычислимых функций замкнут относительно операции подстановки; г) класс* $\mathbf{F}$*-перечислимых множеств замкнут относительно операции пересечения; д)* $B(\mathbf{F})$ *не является* $\mathbf{F}$*-разрешимым.*

ДОКАЗАТЕЛЬСТВО совпадает с соответствующими рассуждениями теории алгоритмов [5].

Для замкнутости указанных классов множеств и предикатов относительно операций проектирования вводятся следующие понятия регулярности и слабой фундированности оракула.

ОПРЕДЕЛЕНИЕ 2. Оракул $\mathbf{F}$ называется регулярным, если существует $\mathbf{F}$-вычислимая функция $v(x,y)$, для которой справедливо соотношение: $\{x,y\} \cap B(\mathbf{F}) \neq \emptyset \to v(x,y)$ определено и принадлежит $\{x,y\} \cap B(\mathbf{F})$.

ТЕОРЕМА 2. *Если оракул* $\mathbf{F}$ *регулярный, то существует* $\mathbf{F}$*-вычислимая функция* μ *(называемая селекторной), которая по* $\mathbf{F}$*-индексу* z *непустого* $\mathbf{F}$*-перечислимого множества дает некоторый элемент* $\mu(z)$ *этого множества.*

Опираясь на эту теорему, легко доказать, что для регулярного оракула $\mathbf{F}$ класс $\mathbf{F}$-перечислимых множеств замкнут относительно операций объединения и проектирования.

Пусть $\mathbf{N} = \{0,1,2,\ldots\}$ и $\overline{\mathbf{N}}$ обозначает множество гёделевских номеров числовых кортежей, и если $u = \langle x_1, \ldots, x_n \rangle$, то $u * m = \langle x_1, \ldots, x_n, m \rangle$, $m * u = \langle m, x_1, \ldots, x_n \rangle$. Непустое множество $\tau \subseteq \overline{\mathbf{N}}$ называется деревом, если выполнено условие: $\langle x_1, \ldots, x_n \rangle \in \tau \rightarrow (\forall i < n) \langle x_1, \ldots, x_i \rangle \in \tau$. Элементы τ называются вершинами дерева, пустой кортеж $\langle\,\rangle$ всегда принадлежат дереву и называется начальной вершиной. Дерево, равное $\{u \in \mathrm{N} \mid m * u \in \tau\}$, если $\langle m \rangle \in \tau$, называется m-й ветвью дерева τ. Пусть для каждой всюду определенной функции α вида $\mathrm{N} \rightarrow \mathrm{N}$ $\bar{\alpha}(n)$ обозначает $\langle \alpha(0), \alpha(1), \ldots$ $\ldots, \alpha(n-1) \rangle$. Дерево τ имеет обрыв цепей, если $(\forall \alpha)$ $(\exists n) \bar{\alpha}(n) \bar{\in} \tau$. Каждому дереву τ с обрывом цепей ставится в соответствие счетный ординал $O(\tau)$ (называемый высотой дерева τ), так что

$$O(\{\langle\,\rangle\}) = 0 \qquad O(\tau) = \sup O(\tau_m) \mid \langle m \rangle \in \tau \},$$

здесь τ_m обозначает m-ю ветвь дерева τ.

Дерево τ называется $\mathbf{F}$-вычислимым, если его характеристическая функция $\mathbf{F}$-вычислима, при этом $\mathbf{F}$-номер этой функции называется $\mathbf{F}$-номером дерева τ.

Введем обозначения: $D(\mathbf{F})$ - множество $\mathbf{F}$-номеров $\mathbf{F}$-вычислимых деревьев; τ_z — $\mathbf{F}$-вычислимое дерево с $\mathbf{F}$-номером z: $b(z,m)$ - рекурсивная функция, равная $\mathbf{F}$-номеру m-й ветви дерева τ_z; $T(\mathbf{F})$ - множество $\mathbf{F}$-номеров $\mathbf{F}$-вычислимых деревьев с обрывом цепей. Для каждого $z \in T(\mathbf{F})$: $|z| = O(\tau_z)$, кроме того, $|T(\mathbf{F})| = \sup\{|z| / z \in T(\mathbf{F})\}$, и если $z \bar{\in} T(\mathbf{F})$, то $|z| = |T(\mathbf{F})|$.

ОПРЕДЕЛЕНИЕ 3. Оракул $\mathbf{F}$ называется слабо фундированнным, если множество $T(\mathbf{F})$ $\mathbf{F}$-перечислимо.

ТЕОРЕМА 3. *Для регулярного слабо фундированного оракула* $\mathbf{F}$: *а) класс* $\mathbf{F}$*-разрешимых предикатов замкнут относительно операций навешивания кванторов;*

б) F *не может быть всюду определенной функцией;*
в) множества $\tilde{B}(F)$, $B^*(F)$, $D(F)$ F*-перечислимы.*

ОПРЕДЕЛЕНИЕ 4. Оракул F называется разложимым по $T(F)$, если существует оператор, который каждому $z \in T(F)$ ставит в соответствие график F_z некоторой функции так, что выполняются следующие условия:

1) $F = \bigcup_{z \in T(F)} F_z$;

2) $(\forall z_1, z_2 \in T(F))\ (|z_1| \leq |z_2| \rightarrow F_{z_1} \subseteq F_{z_2})$;

3) для любого $z \in T(F)$ график F_z является F-разрешимым равномерно по z .

ЛЕММА 1. *Если регулярный слабо фундированный оракул* F *разложим по* $T(F)$ *, то для любого* $z \in B^*(F)$ *существует* x *из* $T(F)$ *такой, что* $z[F] \sim z[F_x]$, *где* F_x *- функции из определения 4 и запись* $z[F] \sim z[F_x]$ *обозначает соотношение:* $(\forall t)\ \{z\}^F(t) = \{z\}^{F_x}(t)$.

ДОКАЗАТЕЛЬСТВО. Пусть F удовлетворяет условию и от противного, существует $z_0 \in B^*(F)$ такой, что для любого $x \in T(F)$ машина z_0 на некотором аргументе с оракулом F вычисляет вопрос y , не принадлежащий δF_x . Каждому $y \in \delta F$ соответствует следующее непустое множество $\{x \in T(F) / y \in \delta F_x\}$. По теореме 3 это множество F-перечислимо равномерно по y, и с помощью F из него можно выбрать некоторый элемент x_y . Пусть ϕ обозначает F-вычислимую функцию, отображающую y в x_y . Тогда график F представим в виде

$$F = \{(x,y)/(\exists t, y')\ [y' - \text{вопрос}\ \langle z_0, t\rangle_F \wedge \wedge F_{\phi(y')}(x) = y]\}. \qquad (1)$$

Действительно, из первого условия разложимости $\mathbf{F}$ следует, что $\mathbf{F}(x) = y \longleftrightarrow (\exists z \in T(\mathbf{F}))\ \mathbf{F}_z(x) = y$. Для z, указанного в правой части этого соотношения, и для выбранного z_0 существует вопрос y' машины z_0 такой, что $y' \overline{\in}\ \delta\mathbf{F}_z$. Для этого y' выполняется неравенство $|z| < |\psi(y')|$, и в силу второго условия разложимости $\mathbf{F}_{\psi(y')}(x) = y$. Обратное очевидно.

По теореме 3 из третьего условия разложимости $\mathbf{F}$ следует $\mathbf{F}$-разрешимость (1), что невозможно. Лемма доказана.

Заметим теперь, что для каждого $z \in T(\mathbf{F})$ множество $\{x \in T(\mathbf{F}) / z[\mathbf{F}] \sim z[\mathbf{F}_x]\}$ непустое и $\mathbf{F}$-перечислимое, его $\mathbf{F}$-индекс находится равномерно по z. В силу регулярности $\mathbf{F}$ существует $\mathbf{F}$-вычислимая функция, которая по z выбирает некоторый элемент x_z этого подмножества.

ЛЕММА 2. *Если регулярный слабо фундированный оракул* $\mathbf{F}$ *разложим по* $T(\mathbf{F})$, *то существует* $\mathbf{F}$*-вычислимая функция* $h(y,z)$ *такая, что для любых* $y \in B^*(\mathbf{F})$, $z \in T(\mathbf{F})$:

$$h(y,z) = \begin{cases} 1, \text{ если } y \in T(\mathbf{F}),\ |y| \le |z|; \\ 0 - \text{в противном случае.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. С помощью теоремы о неподвижной точке строится рекурсивная функция e такая, что для любых $y \in B^*(\mathbf{F})$, $z \in T(\mathbf{F})$: $\{e(z)\}^{\mathbf{F}}(y) = 1$, если $y \in D(\mathbf{F})$ и

$$(\forall n)\ (\{y\}^{\mathbf{F}}(\langle n \rangle) = 1 \to (\exists m)\ (\{z\}^{\mathbf{F}}(\langle m \rangle) = $$
$$= 1 \wedge \{e(b(z,m))\}^{\mathbf{F}}(b(y,n)) = 1)),$$

и $\{e(z)\}^{\mathbf{F}}(y) = 0$ – в остальных случаях.

Так как $y, z \in B^*(\mathbf{F})$, то по теореме 3 предыдущее соотношение $\mathbf{F}$-разрешимо и $\{e(z)\}^{\mathbf{F}}(y)$ определено. Осталось проверить, что $\{e(z)\}^{\mathbf{F}}(y) = h(y,z)$. Это легко осуществляется с помощью индукции по $|z|$. Лемма доказана.

§2. Система $A(F)$

Язык системы $A(F)$ есть язык элементарной арифметики с добавленным к нему функциональным символом оракула F и выделенной предметной константой c, роль которой будет объяснена ниже. При этом к обычным атомным формулам добавляются всевозможные формулы вида $F(t) = s$, где t, s - предметные переменные или константы. Подразумевается, что предметные переменные пробегают натуральный ряд; арифметические операции,отношение равенства и константы имеют свой очевидный смысл, а символ F интерпретируется как некоторая частичная числовая функция.

Известно, что всякие рекурсивные отношения выразимы в языке элементарной арифметики, который полностью содержится в языке системы $A(F)$. Поэтому в $A(F)$ выразимы,например,следующие отношения: "u - гёделевский номер числового кортежа", "z - гёделевский номер машины с оракулом", "машина z вычислила некоторый вопрос". Далее, пусть z - инициальная машина с оракулом, u,v - соответственно номера кортежей $(x_1,\ldots$ $\ldots, x_n),(y_1,\ldots,y_n)$ одинаковой длины. Введем отношение $T(z,t,u,v)$, означающее, что машина z работает t тактов и останавливается, в процессе работы она вычисляет вопросы $x_1,\ldots,x_n$ и получает на них ответы $y_1,\ldots,y_n$ соответственно.Это отношение является рекурсивным и не зависит ни от какого оракула.Если же в описанной здесь ситуации нужно сказать, что z работает с оракулом F, то к отношению $T(z,t,u,v)$ добавляется "формула" $F(x_1) = y_1 \wedge \ldots \wedge F(x_n) = y_n$. Тогда, например, утверждение "машина z с оракулом F останавливается" выразимо формулой:

$$(\exists u,v,t)\ (T(z,t,u,v) \wedge (\forall i \leq lh(u))F((u)_i = (v)_i),$$

где $(u)_i$ - i-я координата кортежа с номером u, $lh(u)$ - длина кортежа u. Конечно, эта формула не является формулой языка $A(F)$, но она составлена из отношений, которые можно выразить в этом языке, поэтому указанное утверждение выразимо в $A(F)$. Аналогично показывается, что множества $B(F)$, $\tilde{B}(F)$, $B^*(F)$, $D(F)$ также выразимы в $A(F)$ (даже, если мы не знаем, что обозначает символ c). Иначе обстоит дело с множеством $T(F)$, так как в его определении фигурирует условие обрыва цепей, обычно описываемое с помощью функциональных кванторов. По этой причине в язык системы $A(F)$ введена константа c , которая будет интерпретироваться как номер машины, F-перечисляющей множество $T(F)$. Тогда, например, отношение "$z \in T(F)$" выражается в $A(F)$ формулой, описывающей отношение "$\langle c, z\rangle \in B(F)$" . Таким образом, заранее предполагается, что будут рассматриваться только такие интерпретации системы $A(F)$, в которых множество $T(F)$ F-перечислимо, т.е. оракул F является слабо фундированным.

Аксиомами системы $A(F)$ являются все аксиомы элементарной арифметики (описывающие свойства арифметических операций, отношений и констант, включая математическую индукцию, распространенную на все формулы $A(F)$), аксиомы исчисления предикатов (описывающие обычные правила рассуждений) и специальные аксиомы (характеризующие символы F и c), перечисленные ниже.

<u>Аксиома однозначности оракула:</u>

$$(F(x) = y \wedge F(x) = z) \rightarrow y = z .$$

<u>Аксиома регулярности оракула</u>: существует F-вычислимая функция (с F-номером v) такая, что $\{x,y\} \cap B(F) \neq \emptyset \rightarrow \{v\}^F(x,y)$ определено и $\in \{x,y\} \cap B(F)$.

<u>Аксиома слабой фундированности оракула</u>: для любого $z \in D(F)$

$$\tau_z = \{\langle\rangle\} \rightarrow \langle c, z\rangle \in B(F) ,$$

$$(\forall n)(b(z,n) \in D(F) \rightarrow \langle c, b(z,n)\rangle \in B(F)) \rightarrow \langle c, z\rangle \in B(F) .$$

Схема аксиом индукции по деревьям:

$$(\forall z\in D(F))[(\tau_z=\{\langle\ \rangle\}\to P(z))\wedge(\forall n)(b(z,n)\in D(F)\to$$
$$\to P(b(z,n)))\ \to P(z)]\to(\forall y)[\langle c,y\rangle\in B(F)\to P(y)]\ ,$$

где P - любая формула рассматриваемого языка.

Аксиома о разложимости оракула: существует рекурсивная функция $m(z)$ такая, что для любого $z\in T(F)$ $m(z)$ есть F-номер характеристической функции графика F_z некоторой функции, так что выполняются:

1) $F=\bigcup\limits_{z\in T(F)} F_z$;

2) $(\forall z_1,z_2\in T(F))(|z_1|\le|z_2|\to F_{z_1}\subseteq F_{z_2})$.

Ясно, что в системе $A(F)$ выразимы почти все введенные ранее понятия. Например, соотношения $z[F]\sim z[F_x]$, $z\in B^*(F_x)$ выражаются через отношение "$\{z\}^{F_x}(t)$ определено", а это отношение может быть описано следующей формулой:

$$(\exists u,v,s)\ (T(\langle z,t\rangle,s,u,v)\wedge$$
$$\wedge(\forall i\le lh(u))\{m(x)\}^F(\langle(u)_i,(v)_i\rangle)=1),$$

которая выразима в $A(F)$.

По построению в любой подразумеваемой интерпретации системы $A(F)$ оракул F является регулярным, слабо фундированным и разложимым по $T(F)$. Поэтому в $A(F)$ доказуемы все предыдущие утверждения, применяющие обычные логические средства (без привлечения трансфинитной индукции). Но конструкции, использующие понятие ординала, требуют дополнительного обоснования в $A(F)$, ибо в ней должны рассматриваться лишь F-вычислимые ординалы, являющиеся высотами F-вычислимых деревьев. Построение функции $h(y,z)$ в первой части доказательства леммы 2 осуществлялось без помощи трансфинитной индукции, и потому оно осуществимо в $A(F)$. Тогда для любых $y, z \in T(F)$ отношения $|y| \leq |z|$ и $|y| < |z|$ выразимы в $A(F)$ соответственно формулами $h(y,z) = 1$ и $h(z,y) = 0$. Но чтобы применять так определенные отношения, надо убедиться, что в $A(F)$ доказуемы их естественные свойства, например, такие, как

$$(|y| \leq |z| \vee |z| \leq |y|),$$

$$(|x| \leq |y| \wedge |y| \leq |z|) \to |x| \leq |z|,$$

$$(|x| < |y| \wedge |y| \leq |z|) \to |x| < |z|,$$

не существует бесконечной последовательности деревьев такой, что $|z_1| > |z_2| > |z_3| > \ldots$

Чтобы проверить эти свойства, достаточно сначала доказать с помощью индукции по деревьям следующие утверждения:

1) если $\tau_y = \{\langle\,\rangle\}$, то $(\forall x \in T(F))\{e(x)\}^F(y) = 1$;

2) если $\{e(x)\}^F(y) = 0$, то $\{e(y)\}^F(x) = 1$;

3) если $\{e(x)\}^F(y) = 0$, то

$$(\exists n)(\{y\}^F(\langle n\rangle) = 1 \wedge \{e(b(y;n))\}^F(x) = 1),$$

где e - функция из доказательства леммы 2. Оставляем это читателю в качестве упражнения.

Теперь эти свойства позволяют нам обосновывать в $A(F)$ необходимые разновидности принципа трансфинитной индукции, используемые в некоторых рассуждениях.

ЛЕММА 3. *В* $A(F)$ *можно обосновать следующий принцип* $|z|$*-индукции. Пусть* $P(z)$ *- произвольная формула из* $A(F)$. *Тогда если для любого* $z \in T(F)$ *выполняется:*

$$\left.\begin{array}{r} (|z| = 0 \to P(z)), \\ (\forall y \in T(F))\,(|y| < |z| \to P(y)) \to P(z), \end{array}\right\} \qquad (2)$$

то $P(z)$ *верна для всех* $z \in T(F)$.

ДОКАЗАТЕЛЬСТВО. Пусть $P(z)$ - формула системы $A(F)$, построим новую формулу $Q(z)$ (из $A(F)$):

$$Q(z) \leftrightarrow (P(z) \wedge (\forall y \in T(F)) (h(z,y) = 0 \to P(y))).$$

Теперь пусть выполняется (2), покажем, что для всех z из $T(F)$ выполняется формула $Q(z)$, а значит, и $P(z)$. Сначала докажем, что если $z, z' \in T(F)$ и $|z'| \le |z|$, то $Q(z)$ влечет $Q(z')$. Действительно, пусть $|z'| \le |z|$ и $Q(z)$ истинна, тогда из последнего следует, что для любого $y \in T(F)$: $|y| < |z'| \to P(y)$. В силу (2) это влечет $P(z')$, а значит, и $Q(z')$.

Далее, доказательство использует индукцию по деревьям. Если $\tau_z = \{\langle\,\rangle\}$, то, в силу (2). $Q(z)$ выполняется. Предположим, что $(\forall n)(b(z,n) \in D(F) \to Q(b(z,n)))$, требуется доказать $Q(z)$. Для этого воспользуемся условием (2). Пусть $y \in T(F)$ и $|y| < |z|$. Тогда согласно предыдущим замечаниям существует $\langle n \rangle \in \tau_z$ такое, что $|y| \le |b(z,n)|$. По предположению $Q(b(z,n))$ верно, а из него в силу предыдущего утверждения следует $Q(y)$, что влечет $P(y)$. Таким образом, $(\forall y \in T(F)) (|y| < |z| \to P(y))$. Из (2) следует, что $P(z)$, а значит, и $Q(z)$ верны. Лемма доказана.

§3. Обобщенно-конструктивный континуум

Пусть зафиксирована гёделевская нумерация всех рациональных чисел, причем каждое натуральное число n является номером некоторого рационального числа r_n. Тогда любая одноместная всюду определенная функция α определяет бесконечную последовательность рациональных чисел $r_{\alpha(0)}, r_{\alpha(1)}, \ldots$ А если такая последовательность сходится, то функция α задает вещественное число, равное $\lim\limits_{t \to \infty} r_{\alpha(t)}$. Вещественное число β называется F-вычислимым, если существует $a \in B^*(F)$ такое, что

$$(\forall m)\ (\exists t_m)\ (\forall t', t'' \geq t_m)\ (|a(t')-a(t'')| < 2^{-m})$$

и $\beta = \lim\limits_{t \to \infty} a(t)$, где $a(t)$ обозначает рациональное число с гёделевским номером $\{a\}^F(t)$. Номер машины a называется кодом β . Пусть Γ - множество всех F-вычислимых вещественных чисел и $\tilde{\Gamma}$ - множество их кодов. Γ называется обобщенно-конструктивным континуумом, а его элементы будем называть точками Γ . Коды a , b одной и той же точки считаются эквивалентными, обозначение: $a \sim b$. Обобщенно-конструктивные функции и множества в Γ определяются следующим образом. Будем говорить, что машина q задает F-конструктивную функцию, если

$$(\forall a \in \tilde{\Gamma})(\{q\}^F(a) \text{ определено } \to \{q\}^F(a) \in \tilde{\Gamma}),$$

$$(\forall a, b \in \tilde{\Gamma})\ (\{q\}^F(a), \{q\}^F(b) \text{ определены и }$$

$$a \sim b \to \{q\}^F(a) \sim \{q\}^F(b)).$$

Эти условия естественным образом определяют функцию на точках Γ . Второе условие означает, что машина q коды одной и той же точки переводит в коды также одной точки. Поэтому если q задает F-конструктивную функцию f , то отношение " f определена в точке α " означает, что для некоторого кода a точки α $\{q\}^F(a)$ определено.

Пусть $M \subseteq \Gamma$ и $\tilde{M}$ - множество всех кодов точек из M. Будем говорить, что M - F-конструктивное множество, если его характеристическая функция F-конструктивна.

Тем самым определена некоторая модель языка классического анализа. Ясно, что введенные понятия выразимы в $A(F)$. Определим канонические коды точек Γ . Пусть $z \in \tilde{\Gamma}$, по лемме 1, существует $x \in T(F)$, для которого $z[F] \sim z[F_x]$, и такой x можно вычислить с помощью F по z ; более того, этот x можно выбрать так, что для любой вершины

$\langle n\rangle \in T_x$ не выполняется соотношение $z[F] \sim z[F_{b(z,n)}]$. Обозначим выбранный таким образом x через x_z, и пусть

$$C_z = \{z' \in B^*(F_{x_z}) / \ z'[F] \sim z[F]\}.$$

В силу разложимости F это множество является F-разрешимым, и, следовательно, с помощью F из него можно выбрать элемент z', у которого соответствующий элемент $x_{z'}$ имеет наименьший ранг $|x_{z'}|$ (последнее записывается следующей формулой: $(\forall y)\ (y \in C_z \to |x_{z'}| \le |x_y|)$, причем эта формула выразима в $A(F)$ и определяет F-разрешимое отношение). Если таких z' несколько, то берется наименьшее из них. Выбранное z' называется каноническим кодом и обозначается $c(z)$. Построенная функция $z \to c(z)$ является F-вычислимой и удовлетворяет условиям:

1) $(\forall z)\ (z \in \tilde{\Gamma} \to c(z)$ определено и $c(z) \sim z)$;

2) $(\forall z_1, z_2 \in \tilde{\Gamma})\ (z_1 \sim z_2 \to c(z_1) = c(z_2))$.

Действительно, пусть $z_1, z_2 \in \tilde{\Gamma}$ и $z_1 \sim z_2$. Им соответствуют $x_1, x_2 \in T(F)$ такие, что $z_1[F_{x_1}] \sim z_2[F_{x_2}]$. Пусть, для определенности, $|x_1| \le |x_2|$. Тогда в силу разложимости $F_{x_1} \subseteq F_{x_2}$ и поэтому $B^*(F_{x_1}) \subseteq B^*(F_{x_2})$. Следовательно, множества C_{z_1} и C_{z_2} имеют одинаковые z' с наименьшим $|x_{z'}|$, значит, $c(z_1) = c(z_2)$, что и требовалось доказать.

Пусть C обозначает множество канонических кодов точек Γ: $C = \{c(z) / z \in \tilde{\Gamma}\}$. Значение $c(z)$ выбирается так, что для некоторого $x_z \in T(F)$ выполняется эквивалентность $c(z)[F] \sim c(z)[F_{x_z}]$. Согласно отмеченным на с. 144 свойствам оракула F в системе $A(F)$ можно доказать, что ординал $|x_z|$ является наименьшим в данной ситуации. Этот орди -

нал принимается за ранг канонического кода: $r(c(z)) = |x_z|$. Тогда множество C вполне упорядочено отношением $r(y) < r(z)$. Распространим это отношение на все натуральные числа: если $z \bar{\in} C$, то для любого $y \in C$ полагаем $r(y) < r(z)$, и если $y, z \bar{\in} C$, то $r(y) < r(z)$ неверно.

ЛЕММА 4. *Если* $z \in C$, *то отношение* $r(y) < r(z)$ F*-разрешимо равномерно по* z.

ДОКАЗАТЕЛЬСТВО. Если $z \in C$, то с помощью F можно вычислить соответствующий ему $x_z \in T(F)$. Теперь, в силу указанных на с.144 свойств, если $r(y) < r(z)$, то для некоторой вершины $\langle n \rangle \in \tau_{x_z}$ выполняется $y[F] \sim y[F_{b(x_z, n)}]$. В силу разложимости оракула это отношение является F-разрешимым по z. Теперь, перебирая все $\langle n \rangle \in \tau_{x_z}$, можно с помощью F проверить истинность отношения $r(y) < r(z)$, что и требовалось доказать.

В связи с введенным понятием необходимо сделать одно замечание технического характера. Пусть машина q задает F-конструктивную функцию, определенную на F-конструктивном множестве M. Тогда для любой $\alpha \in M$ найдется код a точки α, для которого значение $\{q\}^F(a)$ определено. Стало быть, следующее множество непусто и очевидно является F-перечислимым:

$$\{a \in \tilde{\Gamma} \mid a \sim a' \wedge \{q\}^F(a) \text{ определено }\},$$

где a' - канонический код α. F-индекс этого множества находится эффективно по a', q. Пусть машина q' на каноническом коде a' с помощью селекторной функции μ выбирает элемент a указанного множества и вычисляет код $c(\{q\}^F(a))$. Тогда q' определена на всех канонических кодах a' из $\tilde{M} \cap C$, ее значения принадлежат C и она задает ту же F-конструктивную функцию, что и машина q. Очевидно, что q' находится эффективно по q, поэтому в дальнейшем работу таких машин можно рассматривать только на канонических кодах.

ОПРЕДЕЛЕНИЕ 5. Пусть M_1 и M_2 – F-конструктивные множества. Тогда M_1 равномощно M_2 в Γ, если существует F-конструктивная функция φ, которая отображает M_1 на M_2 взаимно-однозначно. Бесконечное F-конструктивное множество называется счетным в Γ, если оно равномощно N в Γ, в противном случае оно называется несчетным в Γ.

ТЕОРЕМА 4. *Для того чтобы бесконечное F-конструктивное множество M было счетным в Γ, необходимо и достаточно, чтобы отношение $x \in \tilde{M} \cap C$ было F-разрешимым.*

ДОКАЗАТЕЛЬСТВО. Пусть F-конструктивное множество M счетно в Γ и машина q вычисляет взаимно-однозначное отображение $\tilde{N} \cap C$ на $\tilde{M} \cap C$. Тогда

$$x \in \tilde{M} \cap C \longleftrightarrow (\exists n \in \tilde{N} \cap C)\{q\}^F(n) = x.$$

По каждому натуральному числу n эффективно строится некоторый его код n', а затем с помощью F можно вычислить его канонический код $c(n')$ и проверить отношение $\{q\}^F(c(n')) = x$. По теореме 3 отсюда следует F-разрешимость $x \in \tilde{M} \cap C$. Обратно, если отношение $x \in \tilde{M} \cap C$ F-разрешимо, то существует машина, которая с оракулом F вычисляет взаимно-однозначное отображение $\tilde{M} \cap C$ на N. Тогда M является счетным в Γ. Теорема доказана.

Заметим, что множество C не является F-разрешимым. Доказательство предоставляется читателю в качестве упражнения. Из этого следует, что весь континуум Γ несчетен в Γ. Следующая теорема утверждает выполнение в Γ аналога континуум-гипотезы. Но для доказательства ее необходимо обосновать в $A(F)$ индукцию по рангу.

ЛЕММА 5. *В $A(F)$ можно обосновать следующий принцип индукции по рангам $r(z)$. Пусть $P(z)$ – некоторая формула системы $A(F)$ и для любого $z \in C$ выполняется:*

$$\left.\begin{array}{r} r(z) = 0 \to P(z), \\ (\forall y \in C)\ (r(y) < r(z) \to P(y)) \to P(z). \end{array}\right\} \qquad (3)$$

Тогда $P(z)$ верна для всех $z \in C$.

ДОКАЗАТЕЛЬСТВО. Пусть $P(z)$ - формула системы $A(F)$, $z \in C$; построим новую формулу $Q(w)$ для $w \in T(F)$:

$$Q(w) \longleftrightarrow (\forall y \in C)\ (r(y) \le |w| \to P(y)).$$

Заметим, что для $y \in C$ и $w \in T(F)$ отношение $r(y) \le |w|$ задается формулой $|x_y| \le |w|$, которая выразима в $A(F)$ в силу F-вычислимости введенных ранее функций $z \to x_z$ и $h(y,z)$.

Теперь пусть выполняется (3). Покажем, что для всех $w \in T(F)$ выполняется $Q(w)$ и, значит, для всех $z \in C$ выполняется $P(z)$. Воспользуемся индукцией по деревьям. Если $\tau_w = \{\langle\ \rangle\}$, то для любого $y \in C$ $r(y) \le |w|$ влечет $r(y) = 0$ и, в силу (3), $P(y)$ истинна, поэтому и $Q(w)$ истинна. Предположим, что

$$(\forall n)\ (b(w,n) \in D(F) \to Q(b(w,n))). \qquad (4)$$

Требуется доказать $Q(w)$. Для этого воспользуемся (3) и некоторыми соотношениями, указанными на с.144.

Пусть $y \in C$ и $r(y) < |w|$, тогда существует вершина $\langle n \rangle \in \tau_w$ такая, что $r(y) \le |b(w,n)|$. В силу предположения (4) для такого n $Q(b(w,n))$ верна и, следовательно, $P(y)$ верна. Таким образом, для любого $z \in C$ если $r(z) \le |w|$, то выполняется $(\forall y \in C)\ (r(y) < r(z) \to P(y))$. Тогда в силу (3) выполняется $P(z)$, а это влечет выполнение $Q(w)$. Лемма доказана.

ТЕОРЕМА 5. *Пусть* $\mathbf{M}$ *- бесконечное* $\mathbf{F}$*-конструктивное множество, несчетное в* Γ*, тогда оно равномощно* Γ.

ДОКАЗАТЕЛЬСТВО. Заметим, что отношение равномощности в Γ коммутативно, поэтому мы будем строить с помощью теоремы о неподвижной точке (которая очевидно выполняется в $A(F)$) общерекурсивную функцию e такую, что функция $\varphi(x)$, равная $\{e(x)\}^F(0)$, отображает множество C на $\tilde{M}\cap C$ взаимно-однозначно и с сохранением отношения $r(x) < r(y)$. Для произвольного $x\in C$ значение $e(x)$ есть номер машины W, которая на аргументе 0 вычисляет F-индекс следующего F-перечислимого множества M_x и с помощью селекторной функции μ выбирает элемент такого множества:

$$M_x = \{z\in \tilde{M}\cap C/(\forall y\in C)\ (r(y) < r(x) \to$$

$$\to \{e(y)\}^F(0) \neq z)\wedge(\forall t\in \tilde{M}\cap C)\ (r(t) < r(z) \to$$

$$\to (\exists y'\in C)\ (r(y') < r(x)\wedge\{e(y')\}^F(0) = t))\}.$$

Так как для любого $x\in C$ отношение $r(y)< r(x)$ F-разрешимо, то указанные в правой части M_x соотношения F-разрешимы, а само M_x F-перечислимо и его F-индекс находится равномерно по X. Далее, M_x состоит из одного элемента z, который не имеет прообраза в множестве $\{y\in C\,|\,r(y)<r(x)\}$ при отображении $\varphi: y\to\{e(y)\}^F(0)$ и обладает наименьшим рангом $r(z)$ среди таких же элементов. Множество M_x не может быть пустым, ибо в противном случае множество $\tilde{M}\cap C$ совпадало бы с F-разрешимым множеством: $\{\{e(y)\}^F(0)\,|\,y\in C\wedge r(y)< r(x)\}$, что невозможно в силу несчетности M. Поэтому функция φ действительно определена для всех $x\in C$, отображает C в $\tilde{M}\cap C$ взаимно-однозначно и с сохранением отношения $r(x) < r(y)$. Строгое доказа -

тельство этих утверждений осуществляется с помощью $r(z)$-индукции, которая обоснована в лемме 5.

Кроме того, φ отображает C на все множество $\tilde{M} \cap C$. Действительно, пусть z - элемент $\tilde{M} \cap C$, не имеющий прообраза в множестве C и обладающий минимальным рангом $r(z)$ среди таких же элементов. Тогда φ взаимно-однозначно отображает C на множество $\{x \in \tilde{M} \cap C \mid r(x) < r(z)\}$, которое F-разрешимо и по теореме 4 соответствует счетному F-конструктивному множеству. Это противоречит несчетности Γ. Следовательно, φ отображает C на все $\tilde{M} \cap C$, и потому M равномощно Γ. Теорема доказана.

Литература

1. ГАНОВ В.А. Обобщенно-конструктивный континуум // Сиб. мат.журн.-1973. - Т.14, № 5. -С. 957-977.

2. ПЛОТНИКОВА Н.А. О вычислениях с оракулами //Сиб. мат. журн.-1983.- Т. 24, № 1. -С. 146-151.

3. ГАМОВА А.Н. Обобщенные вычисления с оракулами //Алгебра и логика. - 1988. - Т. 27, №2. -С. 131-147.

4. БЕЛЯКИН Н.В. Вычисления с оракулами: аксиоматическая версия //Всесоюз.конф. "Применение методов математической логики": Тез.докл. -Таллинн, 1986. -С. 32-36.

5. РОДЖЕРС Х. Теория рекурсивных функций и эффективная вычислимость. - М.: Мир, 1972.

Поступила в ред.-изд.отд.

23 апреля 1990 года