Автор выражает благодарность Я.М.Барздиню за постановку проблемы, а также другим участникам семинара по теории алгоритмов за внимание к работе.

ЛИТЕРАТУРА

1. Buchberger B. Certain decompositions of Gödel numberings and the semantics of programming languages.- International Symposium on Theoretical Programming. Springer-Verlag. Berlin et al, 1974.

2. Мальцев А.И. Алгоритмы и рекурсивные функции.М.,1965.

ТЕОРЕМА О ДВОЙНОЙ НЕПОЛНОТЕ

К.М.Подниэкс

1. Идея изучать теорию-объект в формализованной метатеории принадлежит, по-видимому, П.Лоренцену (см.[I]). Интересное применение этой идеи демонстрирует А.Мостовский [2] : изучение теории множеств ZF (как объекта) в теории классов Морса.

В настоящей статье формализованные метатеории рассматриваются со стороны их неполноты. В метатеории, которая сильнее теории-объекта, иногда можно доказать непротиворечивость последней, но ни в одной фиксированной метатеории нельзя доказать неразрешимость всех "действительно" неразрешимых предложений (достаточно сильной) теории-объекта. С точки зрения такой метатеории можно различить четыре типа предложений теория-объекта: доказуемые, опровержимые, "доказуемо неразрешимые" и "недоказуемо неразрешимые". С точки зрения обычной интуитивной метатеории последние два типа совпадают. Все дело в том, что множество всех неразрешимых предложений, как правило, не является рекурсивно перечислимым.

Как известно, неразрешимую формулу Геделя можно рассматривать как модель классической антиномии Лжец.

p : p ложно

Предложение p , утверждающее собственную ложность, заставляет прибавить к модусам "истинно-ложно" третий модус: "не имеет значения истинности", "неопределенно", "неразрешимо". Введение нового модуса исключает обычные антиномии, но приводит к появлению новых.

q : q ложно или q не имеет значения истинности. Это т.н. Усиленный Лжец, здесь: q истинно влечет q ложно, q ложно влечет q истинно, если q не имеет значения истинности, то q истинно. Если Лжец - антиномия двузначной логики, то Усиленный Лжец - антиномия трехзначной, и для ее "решения" нужно ввести четвертое значение истинности, например, "неразрешимость q неразрешима". Но это тоже не предел... (Идея многозначных антиномий легко усматривается также в антиномии Помешанный Артур из [3].)

В настоящей статье антиномии:

q : q ложно или q неразрешимо,
r : r ложно или r неразрешимо или неразрешимость r неразрешима,
s : и т.д.

используются для построения "более чем неразрешимых" формул теории-объекта. Пусть T -теория, Q -ее метатеория. Неразрешимая формула Геделя как бы утверждает "я невыводима в T". Еще более неразрешимой будет формула, утверждающая,"в T выводимо мое отрицание или в Q доказуема моя неразрешимость".

2. А п п а р а т. Ради простоты изложения рассматриваются только рекурсивно аксиоматизированные теории первого порядка (с равенством) на языке формальной арифметики [4].

Теорию Q будем называть м е т а т е о р и е й теории T, если в Q выражено понятие о T -доказательстве. Более точно, во-первых, фиксировано рекурсивное $1-1$ -отображение формул и T -доказательств в натуральные числа (образы называются Q -и м е н а м и). Во-вторых, фиксированы формулы $Prf_T^{(Q)}(x,y)$, $Prf\ Neg_T^{(Q)}(x,y)$ со свободными x, y такие, что:

а) если n -имя T -доказательства формулы с именем m, то $\vdash_Q Prf_T^{(Q)}(\bar{m},\bar{n})$, в противном случае $\vdash_Q \neg Prf_T^{(Q)}(\bar{m},\bar{n})$.

б) если n -имя T -доказательства о т р и ц а н и я формулы с именем m то $\vdash_Q Prf\ Neg_T^{(Q)}(\bar{m},\bar{n})$, в противном случае $\vdash_Q \neg Prf\ Neg_T^{(Q)}(\bar{m},\bar{n})$.

Утверждение о том, что формула с Q -именем доказуема, опровержима или разрешима в T, можно выразить формулами:

$$Pr_T^{(Q)}(x) \equiv (\exists y)\ Prf_T^{(Q)}(x,y),$$

$$Pr\ Neg_T^{(Q)}(x) \equiv (\exists y)\ Prf\ Neg_T^{(Q)}(x,y),$$

$$Dec_T^{(Q)}(x) \equiv (\exists y)[\ Prf_T^{(Q)}(x,y) \vee Prf\ Neg_T^{(Q)}(x,y)].$$

Теорию T будем называть ω^k -н е п р о т и в о р е ч и в о й $(0 < k < \omega)$, если для любой формулы $\mathfrak{A}$ следующие утверждения несовместимы

(а) $\vdash_T \neg \mathfrak{A}(\bar{n}_1,\dots,\bar{n}_k)$ для всех наборов $n_1 \dots n_k$

(б) $\vdash_T (\exists x_1 \dots \exists x_k)\ \mathfrak{A}(x_1 \dots x_k)$.

При $k=0$ получается понятие (простой) непротиворечивости. Если в T выводимы все аксиомы формальной арифметики [4], то при $k \geq 1$ ω^k-непротиворечивость равносильна ω -непротиворечивости. Наиболее естественным является, конечно, понятие $\exists$ -н е п р о т и в о р е ч и в о с т и (конъюнкция всех ω^k).

ЛЕММА 1. Пусть Q -метатеория теории
(1) Если m -имя формулы, разрешимой в

$\vdash_Q Dec_T^{(Q)}(\bar{m})$.

(2) Если $\vdash_Q Dec_T^{(Q)}(\bar{m})$ и теория Q ω-непротиворечива, то формула с именем m разрешима в T.

(3) То же для формул Pr, $Pr\ Neg$.

Теорию T назовем д о с т а т о ч н о с и л ь н о й, если в ней п р е д с т а в и м а любая общерекурсивная функция. Например, в случае 1-местной функции f для всех k, ℓ:

$$f(k)=\ell \quad \text{влечет} \quad \vdash_T (\forall y)[F(\bar{k}, y) \equiv (y=\bar{\ell})].$$

В достаточно сильной теории в ы р а з и м о любое рекурсивное отношение натуральных чисел, например:

$$A(k,\ell,m) \quad \text{влечет} \ \vdash_T \mathfrak{A}(\bar{k}, \bar{\ell}, \bar{m}),$$

$$\neg A(k,\ell,m) \quad \text{влечет} \ \vdash_T \neg\mathfrak{A}(\bar{k},\bar{\ell},\bar{m}).$$

Теория T будет достаточно сильной, если в ней выводимы все аксиомы теории Р.Робинсона [4].

ЛЕММА 2. Пусть формулы $F(x,y)$, $G(x,y)$ представляют в теории T функции f, g, причем $f(k)=\ell$, $g(\ell)=m$. Тогда для любой формулы $\mathfrak{A}$:

$$\vdash_T (\exists y)[F(\bar{k},y) \wedge \mathfrak{A}(y)] \equiv \mathfrak{A}(\bar{\ell}),$$

$$\vdash_T (\exists yz)[F(\bar{k}, y) \wedge G(y,z) \wedge \mathfrak{A}(y,z)] \equiv \mathfrak{A}(\bar{\ell},\bar{m}).$$

3. Т е о р е м а о д в о й н о й н е п о л н о т е. Пусть T - достаточно сильная теория, Q - ее метатеория. Тогда фиксирована формула $Dec_T^{(Q)}(x)$. С другой стороны, предполагая геделевскую арифметизацию T и Q, найдутся формулы $Prf_T^{(T)}(x,y)$, $Prf\ Neg_T^{(T)}(x,y)$, $Prf_Q^{(T)}(x,y)$, $Prf\ Neg_Q^{(T)}(x,y)$, выражающие в теории T понятия о T- и Q-доказательствах. Найдутся также:

(а) формула $Sub^{(T)}(x,y,z)$, представляющая в T функцию $z(x,y)$: "z есть (геделев) номер формулы, полученной из формулы с номером x подстановкой цифры $\bar{y}$ вместо всех свободных переменных",

(б) формула $Sub_*^{(T)}(x, y, z)$, представляющая в функцию "z есть номер формулы, полученной из формулы с номером x подстановкой Q-имени формулы с номером y вместо всех свободных переменных".

"Более чем неразрешимую" формулу теории T мы получим, моделируя антиномию

q : q ложно или q неразрешимо

в виде формулы, утверждающей: "в T выводимо мое отрицание или в Q доказуема моя неразрешимость".

Возьмем следующую формулу $A(x)$:

$$(\exists y z)[Sub_1^{(T)}(x,x,y) \wedge Sub_*^{(T)}(\bar{\mu}, y, z) \wedge$$
$$\wedge (\exists u)(Prf\ Neg_T^{(T)}(y,u) \vee Prf\ Neg_Q^{(T)}(z,y))],$$

где μ - номер формулы $Dec_T^{(Q)}(x)$ со свободной переменной x. Пусть m - номер формулы $A(x)$. Рассмотрим $A(\bar{m})$. По лемме 2 $A(\bar{m})$ эквивалентна

$$(\exists u)[Prf\ Neg_T^{(T)}(\bar{n},u) \vee Prf\ Neg_Q^{(T)}(\bar{\bar{n}}, u)], \qquad (*)$$

где n - номер $A(\bar{m})$, $\bar{n}$ - номер $Dec_T^{(Q)}(\bar{a})$, a - имя $A(\bar{m})$.

ТЕОРЕМА 1 (теорема о двойной неполноте). Пусть T - достаточно сильная теория, Q - ее метатеория. Q-имя (замкнутой) формулы $A(\bar{m})$ обозначим через a.

(1) Если T ω-непротиворечива и Q -(просто) непротиворечива, то $A(\bar{m})$ невыводима в T и $\neg Dec_T^{(Q)}(a)$ недоказуема в Q.

(2) Если T непротиворечива, то $\neg A(\bar{m})$ невыводима в T.

(3) Если T и Q ω-непротиворечивы, то $Dec_T^{(Q)}(a)$ недоказуема в Q ;

ДОКАЗАТЕЛЬСТВО.

(а) Пусть $\vdash_T A(\overline{m})$. Если T , Q непротиворечивы, то не $\vdash_T \neg A(\overline{m})$ и по лемме 1, не $\vdash_Q \neg Dec_T^{(Q)}(\bar{a})$. Поэтому для всех натуральных чисел s :

$$\vdash_T \neg Prf\ Neg_T^{(T)}(\bar{n}, \bar{s}) \wedge \neg Prf\ Neg_Q^{(T)}(\bar{\bar{n}}, \bar{s}).$$

Вместе с (*) это дает ω-противоречие в теории T

(б) Пусть $\vdash_T \neg A(\overline{m})$. Тогда:

$$\vdash_T (\exists z)\ Prf\ Neg_T^{(T)}(\bar{n}, z),$$

т.е. $\vdash_T A(\overline{m})$. Противоречие в теории T .

(в) Пусть $\vdash_Q \neg Dec_Q^{(T)}(\bar{a})$. Тогда:

$$\vdash_T (\exists z)\ Prf\ Neg_Q^{(T)}(\bar{\bar{n}}, \bar{z})$$

т.е. $\vdash_T A(\overline{m})$. См. теперь пункт (а).

(г) Пусть $\vdash_Q Dec_T^{(Q)}(\bar{a})$. Тогда по лемме 1, если Q ω-непротиворечива, то $A(\overline{m})$ разрешима в T . См. теперь пункты (а, б).

Теорема 1 доказана.

4. Выводы.

Итак, если достаточно сильная теория T ω-непротиворечива и выбрана какая-либо непротиворечивая ее метатеория Q , то в T найдется неразрешимое предложение, неразрешимость которого нельзя доказать средствами Q .

Теорему Геделя о неполноте можно истолковать как общее опровержение следующего "закона исключенного третьего": в математике всякая определенная гипотеза будет в конечном счете либо доказана, либо опровергнута, опираясь на традиционные математические представления. В таком случае теорема о двойной неполноте показывает, что нет оснований и для "закона исключенного четвертого": всякая

определенная гипотеза будет в конечном счете либо доказана, либо опровергнута, либо будет доказана ее неразрешимость.

К сожалению, этот вывод не является новым. Неразрешимость гипотезы H можно считать надежно установленной, если в ZFC удалось вывести импликацию

$$Con(ZF) \to Con(ZFC + H) \wedge Con(ZFC + \neg H).$$

Давно известно, что "существует недостижимый кардинал" не является такой гипотезой.

5. Обобщение. Используя многозначные антиномии, приведенные в разделе 1, нетрудно доказать теорему о тройной и вообще любой n-кратной неполноте. Все эти теоремы, а также теорема об ω-кратной неполноте и многие вариации на эту тему, содержатся в теореме 2.

Перечислимо растущее дерево метатеорий, это пара $\Sigma = (\mathfrak{M}, \varphi)$ где

(а) машина $\mathfrak{M}$ перечисляет непустое множество конечных кортежей натуральных чисел, причем так, что кортеж $(n_0\ n_1 \ldots n_k)$ перечисляется только после кортежей Λ, (n_0), $(n_0\ n_1)$, ..., $(n_0\ n_1 \ldots n_{k-1})$. Кортежи будем называть вершинами. Будем говорить, что вершина $(n_0 \ldots n_k)$ непосредственно вырастает из $(n_0 \ldots n_{k-1})$,

(б) ч.р. функция φ соотносит с каждой вершиной Q перечисляемого дерева некоторую теорию вместе с фиксированным способом, делающим Q метатеорией для теории, соотнесенной с вершиной T , из которой Q непосредственно вырастает. Исключение составляет вершина Λ (пустой кортеж), ей φ соотносит теорию-объект. Обозначения вершин и соответствующих теорий не различаются.

Пусть Σ -перечислимо растущее дерево метатеорий над теорией-объектом Λ . С каждой формулой F теории Λ ассоциируется перечислимая система формул $\{Dec_{FT} \mid T \in \Sigma\}$ где $Dec_{F\Lambda} = F$ и если Q непосредственно вырастает из T , то Dec_{FQ} -стандартная формула, утверждающая, что формула Dec_{FT} разрешима в теории T

ТЕОРЕМА 2. Пусть $\sum$ -перечислимо растущее дерево ω -непротиворечивых метатеорий с достаточно сильной ω^2 -непротиворечивой теорией-объектом Λ. Тогда найдется замкнутая формула F теории Λ такая, что для всех $T \in \sum$ формула Dec_{FT} неразрешима в T.

ДОКАЗАТЕЛЬСТВО. Строится формула F, которая утверждает "существует $T \in \sum$ такое, что в T доказуема формула $\neg Dec_{FT}$, где F -это я". Квантор существования играет здесь роль бесконечной дизъюнкции (ср. антиномии в разделе 1). Если дерево $\sum$ имеет только конечное число вершин, достаточно потребовать ω -непротиворечивость теории-объекта Λ. В случае бесконечного $\sum$ нужна ω^2 -непротиворечивость Λ. Если предположить ω^3 -непротиворечивость Λ, доказательство можно провести и без информации о конечности-бесконечности дерева $\sum$.

6. Нерешенные проблемы.

1. Теорему о двойной неполноте легко доказать в следующей немного усиленной форме. Пусть T -достаточно сильная теория, Q -ее метатеория, T и Q ω -непротиворечивы. Найдется замкнутая T -неразрешимая формула (с именем a), для которой в Q недоказуема формула $\neg Pr_T^{(Q)}(\bar{a})$. Это действительно усиление, поскольку Q -недоказуемость $\neg Pr_T^{(Q)}(\bar{a})$ влечет недоказуемость $\neg Dec_T^{(Q)}(\bar{a})$, а недоказуемость $Pr_T^{(Q)}(\bar{a})$, $Pr\ Neg_T^{(Q)}(\bar{a})$, $Dec_T^{(Q)}(\bar{a})$ тривиальна в силу леммы 1. Неизвестно, можно ли обеспечить здесь одновременно Q-невыводимость еще и формулы $\neg Pr\ Neg_T^{(Q)}(\bar{a})$?

II. Пусть теория T (на языке формальной арифметики) $\exists$ -непротиворечива и: (а) в T доказуемы все истинные равенства, не содержащие переменных, (б) в T опро-

вержимы все ложные равенства такого рода. Следуя решению 10-ой проблемы Гильберта [5], можно построить диофантово уравнение $P(x_1 \ldots x_k) = 0$, не имеющее решений в натуральных числах и такое, что формула

$$F \equiv (\forall x_1 \ldots \forall x_k)\ P(x_1 \ldots x_k) \neq 0$$

неразрешима средствами теории T.

Заметим, однако, что в данном случае теория $T + \neg F$ оказывается $\exists$ -противоречивой, тогда как $T + F$, по-видимому, $\exists$ -непротиворечива. Таким образом, альтернатива "F или $\neg F$" не совсем безразлична для теории T, хотя она и неразрешима средствами T.

Возможна ли (замкнутая) формула G такая, что теории $T + G$, $T + \neg G$ обе $\exists$ -непротиворечивы? (Определение $\exists$ -непротиворечивости см. в разделе 2).

III. Теорию T назовем безгранично делимой, если любую независимую ее аксиому можно заменить на две новые аксиомы, не нарушая независимость и не меняя область выводимых формул. Это определение легко уточняется в каждом конкретном случае. Например, в случае исчисления высказываний фиксируются правила вывода: *modus ponens* и правило подстановки. Тогда "проблема деления" рассматривается для любой конечной независимой системы аксиом. Является ли исчисление высказываний безгранично делимым? Возможна ли бесконечная независимая система аксиом для (классического) исчисления высказываний?

IV. Введем в язык формальной арифметики переменную X для множеств натуральных чисел, допуская атомарные формулы вида $t \in X$, где t -произвольный терм. Известно [6], что для любого множества A, перечислимого с оракулом B, найдется формула $F(x, X)$ такая, что для всех n : $n \in A$ если и только если $F(\bar{n}, B)$ -истинная формула. Можно ли обобщить решение 10-ой проблемы Гильберта [5] таким образом, чтобы в качестве всегда получалась формула вида

$$(\exists x_1 \ldots \exists x_k)\, G(x, X, x_1 \ldots x_k),$$

где G не содержит кванторов?

У. В классической арифметике, спекулируя на схеме $A \to (\neg A \to B)$, из любого противоречия легко выводится $0=1$. Осуществим ли такой вывод чисто арифметическими средствами, т.е. не используя $A \to (\neg A \to B)$? Например, $0=1$ арифметически следует из $4=5$ или из $(\exists x)(x=x+1)$. Но следует ли $0=1$ арифметически из любого противоречия $A \wedge \neg A$? Более точно, речь идет о возможности "универсального противоречия" в арифметике, использующей вместо классической логики т.н. минимальную логику [7] (плюс еще, быть может, закон двойного отрицания $\neg\neg \to A$).

ЛИТЕРАТУРА

1. Линдон Р. Заметки по логике. М., 1968.
2. Мостовский А. Конструктивные множества и их приложения. М., 1973.
3. Wormell C. P. On the paradoxes of self-reference, "Mind", 1958, v.67, No 266, pp. 267-271.
4. Мендельсон Э. Введение в математическую логику. М., 1971.
5. Матиясевич Ю.В. Диофантовы множества. -УМН, 1972, т.27, № 5.
6. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М., 1972.
7. Гастев Ю. Минимальная логика. -Философская энциклопедия, т. 3. М., 1964.

БЫСТРЫЕ ВЫЧИСЛЕНИЯ НА ВЕРОЯТНОСТНЫХ МАШИНАХ ТЬЮРИНГА

Р.В.Фрейвалд

Рассматривается обыкновенная одноленточная машина Тьюринга (без входа) с одной головкой на ленте, дополненная датчиком случайных чисел, выдающим символы 0 и 1 с равными вероятностями $\frac{1}{2}$ по бернуллиевской схеме, т.е. независимо друг от друга. Такую машину ниже будем называть вероятностной машиной Тьюринга.

Будем говорить, что вероятностная машина Тьюринга $\mathfrak{M}$ распознает множество A с вероятностью, превосходящей p ($\frac{1}{2} \leq p < 1$) за время $t(x)$, если при работе $\mathfrak{M}$ на произвольном слове x с вероятностью строго большей чем p произойдет следующее событие: машина остановится за не более чем $t(x)$ тактов с результатом

$$C_A(x) = \begin{cases} 1 & \text{, если } x \in A \\ 0 & \text{, если } x \in \bar{A} \end{cases}$$

Будем говорить, что вероятностная машина Тьюринга $\mathfrak{M}$ распознает множество A с вероятностью $1-o(1)$ за время $t(x)$, если для любого $\varepsilon > 0$ существует такое n, что при работе $\mathfrak{M}$ на произвольном слове x, длина которого превосходит n, с вероятностью строго большей чем $1-\varepsilon$ произойдет следующее: машина остановится за не более чем $t(x)$ тактов с результатом $C_A(x)$.

Я.М.Барздинь в [1] в частности доказал, что для любой (детерминированной) машины Тьюринга $\mathfrak{M}$, распознаю-