УДК 517.11:518.5

В.А. Ганов

Вычисления с оракулом и ограничением на диалог

Ключевые слова: машины с оракулом, проблема остановки, перечислимые множества, арифметические множества.
Key words: machine with the oracle, problem of the stop, enumerable sets, arithmetical sets.

Данная работа продолжает исследования, описанные в [1, с. 82]. Здесь рассматриваются вычисления на машинах с оракулом, работающих с ограничением на число вопросов. Предполагается, что любая машина может задавать только конечное, хотя заранее неизвестное число вопросов. Ясно, что если машина останавливается с некоторым результатом, то она задает лишь конечное число вопросов. Поэтому данное ограничение выглядит искусственным, и не следует ожидать, что оно внесет какие-нибудь существенные изменения в класс вычислимых объектов. Но особенность данного ограничения в том, что задаваемые вопросы касаются поведения машин, которые также могут задавать лишь конечное число вопросов, в противном случае оракул на таком вопросе не определен. В результате происходит уменьшение области определения оракула и, следовательно, уменьшение класса функций, вычислимых с таким оракулом.

Чтобы проверить эти предположения, в работе строится оракул F_O, аналогичный гиперарифметическому оракулу из [2, с. 36] и удовлетворяющий рассматриваемому ограничению. Доказывается, что класс F_O-разрешимых и F_O-перечислимых множеств не выходит за рамки известных арифметических множеств. Тем не менее аналоги некоторых важных свойств гиперарифметической вычислимости сохраняются и для вычислений с таким ограничением.

1. Ограничение на диалог машины с оракулом и проблема остановки. Вычисления с оракулами уже достаточно глубоко изучены, поэтому здесь приводятся лишь основные обозначения и некоторые соглашения. Фиксируется геделевская нумерация программ машин с оракулом, и коды машин отождествляются с номерами их программ. Инициальной машиной называется геделевский номер $\langle z, x\rangle$. пары, составленной из кода некоторой одноместной машины z и аргумента x, к которому она применяется. Если $\langle z, x\rangle$ при своей работе задает конечное число вопросов, которые касаются поведения таких же, как она машин, то считается, что $\langle z, x\rangle$ работает с ограничением на диалог. Если машина $\langle z, x\rangle$ вычислила вопрос y, но значение оракула $F(y)$ не определено, то работа этой машины не определена, другими словами, $\langle z, x\rangle$ застревает с оракулом F на вопросе y.

Таким образом, в работе $\langle z, x\rangle$ с оракулом F возможны четыре случая:

1) $\langle z, x\rangle$ останавливается с некоторым результатом;

2) $\langle z, x\rangle$ работает бесконечно, но задает конечное число вопросов и получает на них ответы;

3) $\langle z, x\rangle$ задает бесконечное число вопросов и получает на них ответ;

4) $\langle z, x\rangle$ застревает на некотором вопросе.

В случаях 1, 2 считается, что $\langle z, x\rangle$ хорошо работает с оракулом F, и используется обозначение $<z, x> F_O$. Пусть $\overline{B}_O(F)$ – множество инициальных машин $\langle z, x\rangle$, которые хорошо работают с оракулом F; $F_O\ (F)$ – множество машин $\langle z, x\rangle$ из $\overline{B}_O(F)$, которые останавливаются.

Функция $f(\overline{x})$, вычислимая с оракулом F на машине z, которая на всех допустимых значениях аргументов $\overline{x}$ работает с ограничением на диалог, называется F-вычислимой с ограничением на диалог и обозначается через $\{z\}_O^F(\overline{x})$. При этом z называется F-кодом этой функции. Естественным образом определяются множества и отношения, F-разрешимые с ограничением на диалог, и их F-коды. В дальнейшем в данной работе рассматриваются только вычисления с ограничением на диалог.

Аналогично [2, с. 36] доказывается, что ни с каким оракулом F множество $B_O\ (F)$ не является F-разрешимым. В частности, характеристическая функция этого множества служит примером функции, которая не является F-вычислимой с ограничением на диалог. Тем самым для произвольной инициальной машины $\langle z, x\rangle$ невозможно установить, остановится она или нет. В связи с этим вводится ограниченная проблема остановки, которая ставит вопрос о принадлежности $\langle z, x\rangle$ множеству $B_O\ (F)$ если известно, что $\langle z, x\rangle$ хорошо работает с оракулом F. Оракулы, для которых такая ограниченная проблема остановки является F-разрешимой, широко известны. Но здесь в вычисления внесено необычное ограничение, поэтому целесообразно повторить построение оракула, решающего эту проблему.

Индукцией по индексу n определяется следующая последовательность оракулов:

$$F^0, F^1, \dots , F^n, \dots \quad . \qquad (1)$$

0-й шаг. Пусть $F^0 = \varnothing$. $n + 1$-й шаг. Пусть оракул F^n построен, тогда F^{n+1} есть наименьшая (в смысле графика) функция, удовлетворяющая следующим трем условиям:

1) $F^{n+1}(2^w) = 0$, если $w \in B_O(F^n)$;

2) $F^{n+1}(2^w) = 1$, если $w \in \overline{B}_O(F^n) \setminus B_O(F^n)$;

3) $F^{n+1}(3^{<w_1, w_2>}) = <m, w>$, если $\{w_1, w_2\} \cap \cap \overline{B}_O(F^n) \neq \varnothing$, m – наименьшее число такое, что $\{w_1, w_2\} \cap \overline{B}_O(F^m) \neq \varnothing$ и $w = \min\{w_1, w_2\} \cap \overline{B}_O(F^m)$.

В следующем утверждении показывается, что последовательность (1) и связанные с ней множества хорошо работающих машин монотонно расширяются.

Лемма 1. Для любого n имеют место соотношения:

$$F^n \subseteq F^{n+1} \text{ и } \overline{B}_O(F^n) \subseteq \overline{B}_O(F^{n+1}). \qquad (2)$$

Доказательство. Легко видеть, что первое соотношение в (2) влечет второе. Поэтому пусть $\neg F^n \subseteq F^{n+1}$, и n – наименьшее число с таким свойством. Тогда существует x такой, что $F^n(x)$ определено и не равно $F^{n+1}(x)$. Ясно, что $n \neq 0$, тогда $n = k + 1$. Возможны два случая.

1. Пусть $x = 2^w$и $w \in \overline{B}_O(F^k)$. В силу минимальности n: $F^k \subseteq F^n$, следовательно, $w \in \overline{B}_O(F^n)$ и работа w с оракулом F^n совпадет с работой w с оракулом F^k, и поэтому $F^n(x) = F^{n+1}(x)$. Это противоречит выбору n.

2. Пусть $x = 3^{<w_1, w_2>}$, $F^n(x) = <m, w>$, где m – наименьшее число такое, что $\{w_1, w_2\} \cap \cap \overline{B}_O(F^m) \neq \varnothing$, и $w = \min\{w_1, w_2\} \cap \overline{B}_O(F^m)$. По предположению $F^k \subseteq F^n$, следовательно, $\overline{B}_O(F^k) \subseteq \subseteq \overline{B}_O(F^n)$, и тогда числа m и w удовлетворяют соотношениям, определяющим значение $F^{n+1}(x)$. Поэтому $F^n(x) = F^{n+1}(x)$, что противоречит выбору n. Лемма доказана.

Свойство монотонности последовательности (1) позволяет определить искомый оракул как предел этой последовательности.

Определение 1. Пусть $F_O = \bigcup_n F^n$.

Очевидно, что для каждого числа n: $F^n \subseteq F_O$. Отсюда следует, что $\overline{B}_O(F^n) \subseteq \overline{B}_O(F_O)$. Кроме того, работа любой инициальной машины с оракулом F_O совпадает с работой этой же машины с некоторым оракулом F^n. Следовательно, верны равенства: $B_O(F_O) = \bigcup_n B_O(F^n)$ и $\overline{B}_O(F_O) = \bigcup_n \overline{B}_O(F^n)$. Тогда оракул F_O есть наименьшая числовая функция, удовлетворяющая следующим условиям:

1) $F_O(2^w) = 0$, если $w \in B_O(F_O)$;

2) $F_O(2^w) = 1$, если $w \in \overline{B}_O(F_O) \setminus B_O(F_O)$;

3) $F_O(3^{<w_1, w_2>}) = <m, w>$, если $\{w_1, w_2\} \cap \cap \overline{B}_O(F_O) \neq \varnothing$, m – наименьшее число такое, что $\{w_1, w_2\} \cap \overline{B}_O(F^m) \neq \varnothing$.

В остальных случаях значения оракула F_O не определены. Первые два условия означают, что F_O решает проблему остановки для машин, хорошо работающих с ним же. Можно заметить, что, по сравнению с гиперарифметическим оракулом, это свойство более слабое, так как оно не охватывает инициальные машины, задающие бесконечное число вопросов. На первый взгляд это ослабление не является значительным, но оказывается наоборот, класс F_O-разрешимых множеств существенно сужается и не выходит за пределы класса арифметических множеств. Более того, исчезают основные свойства гиперарифметического оракула, связанные с принципами замкнутости класса F_O-перечислимых множеств. И чтобы восполнить такое ослабление, в определение оракула F_O введено третье условие, обеспечивающее существование следующей F_O-вычислимой функции $v(w_1, w_2)$, которая называется парной селекторной функцией.

Лемма 2. Существует F_O-вычислимая функции $v(w_1, w_2)$ такая, что, если $\{w_1, w_2\} \cap B_O(F_O) \neq \varnothing$, то $v(w_1, w_2) \in \{w_1, w_2\} \cap B_O(F_O)$.

Доказательство. Искомая функция $v(w_1, w_2)$ есть результат следующей процедуры. По аргументам w_1, w_2 строится вопрос $3^{<w_1, w_2>}$ оракулу. Если получен ответ $F_O(3^{<w_1, w_2>}) = <m, w>$, то строится вопрос 2^w. Если ответ $F_O(2^w) = 0$, то результат процедуры равен w. В остальных случаях данная процедура не определена. Из определения F_O следует, что эта процедура F_O-вычислима и $v(w_1, w_2)$ удовлетворяет утверждению леммы.

2. Основные принципы программирования. Как уже отмечалось выше, класс F_O-вычислимых функций замкнут относительно арифметических действий и операции суперпозиции. Это влечет замкнутость класса F_O-разрешимых множеств относительно основных теоретико-множественных операций. И эти утверждения выполняются равномерно по F_O-кодам соответствующих F_O-вычислимых объектов. При этом вычисления с оракулом F_O удовлетворяют ограничению на диалог. Теперь, аналогично известным утверждениям теории рекурсивных функций, доказываются следующие ограниченные аналоги S-m-n-теоремы и теоремы о неподвижной точке.

Теорема 1. 1. Существует рекурсивная функция $S_1^1(z, y)$ такая, что если z – F_O-код F_O-вычислимой функции $\{z\}_O^{F_O}(y, x)$, то выполняется соотношение:

$$(\forall x)[\{S_1^1(z, y)\}_O^{F_O}(x) \cong \{z\}_O^{F_O}(y, x)].$$

2. Для любой F_O-вычислимой функции $g(z,x)$ существует F_O-код z_0 такой, что имеет место следующее соотношение: $(\forall x)[\{z_0\}_O^{F_O}(x) \cong g(z_0,x)]$.

3. Арифметичность вычислений с ограничением на диалог. Ниже показывается, что F_O-разрешимые множества являются арифметическими множествами в смысле арифметической иерархии числовых множеств из [3, с. 387].

Вводится следующая процедура. Конечное множество D_u с кодом u называется указателем, если оно состоит из пар вида $(2^w,\ y)$ и $(3^w,\ y)$ и не содержит различных пар с одинаковыми левыми частями. Производится моделирование работы машины $\langle z,\ x\rangle$ по ее программе, за исключением тех моментов, когда она задает вопросы. Если $\langle z,\ x\rangle$ задала вопрос 2^w или 3^w и соответствующая пара – $(2^w,\ y)$ или $(3^w,\ y)$ – входит в указатель D_u, то машине $\langle z,\ x\rangle$ дается ответ y и продолжается ее моделирование. Если такой пары в D_u нет, то моделирование $\langle z,\ x\rangle$ прекращается и выдается символ $\varnothing$. Так как D_u – конечное множество, то описанная процедура является рекурсивной относительно D_u. Вводится предикат $T(z, x, t, w, u)$, который истинен, если $\langle z,\ x\rangle$ и D_u удовлетворяют указанным условиям и описанная процедура моделирования $\langle z,\ x\rangle$ с указателем D_u заканчивается за t тактов с результатом w, а в остальных случаях этот предикат ложен. Так как моделирование $\langle z,\ x\rangle$ производится не более t тактов, то $T(z, x, t, w, u, v)$ – рекурсивный предикат.

Лемма 3. Для любого n отношения $F^n(x) = y$, $w \in B_O(F^n)$, $w \in \overline{B}_O(F^n)$ являются арифметическими.

Доказательство (индукцией по n). Случай $n = 0$ очевиден. Пусть $n = k + 1$, и для любого $m \le k$ отношения $F^m(x) = y$, $w \in B_O(F^m)$, $w \in \overline{B}_O(F^m)$ – арифметические. Отношение $F^{k+1}(x) = y$ означает следующее: либо

$$x = 2^w \wedge [(y = 0 \wedge w \in B_O(F^k)) \vee$$
$$(y = 1 \wedge w \in \overline{B}_O(F^k) \backslash B_O(F^k))];$$

либо

$$x = 3^{<w_1,\, w_2>} \wedge y = \ <m, w> \wedge$$
$$(m - \textit{наименьшее число такое, что}$$
$$(m \le k \wedge \ (w_1 \in \overline{B}_O(F^m) \vee \ w_2 \in \overline{B}_O(F^m))) \wedge$$
$$w = \min\{w_1, w_2\} \cap \overline{B}_O(F^m)\ .$$

Согласно индукционному допущению, с помощью известного алгоритма Тарского-Куратовского доказывается, что это отношение является арифметическим. Отношения $< z, x > \in B_O(F^{k+1})$, $< z, x > \in \overline{B}_O(F^{k+1})$ означают следующее:

1) существует число u такое, что конечное множество D_u с кодом u состоит из пар вида $(2^w,\ y)$ и $(3^w,\ y)$, удовлетворяющих условиям $F^k(2^w) = y$ и $F^k(3^w) = y$ соответственно;

2) машина $< z, x >$ получает ответы на все свои вопросы при ее моделировании с указателем D_u ;

3) для истинности отношения $< z, x > \in B_O(F^{k+1})$ дополнительно должно выполняться условие: $(\exists t, w)\ T(z, x, t, w, u)$.

Как и в предыдущем случае, доказывается, что эти отношения – арифметические. Лемма доказана.

Непосредственным следствием этой леммы являются следующие утверждения.

Теорема 2. Множества $B_O(F_O)$ и $\overline{B}_O(F_O)$ суть арифметические.

Теорема 3. Каждое F_O-разрешимое множество – арифметическое.

Но утверждение, обратное теореме 3, не является верным. Действительно, согласно замечанию, сделанному в начале пункта 1, арифметические множества $B_O(F_O)$ *и* $\overline{B}_O(F_O)$ не являются F_O-разрешимыми.

4. Перечислимые множества. Теперь вполне естественным выглядит желание рассмотреть F_O-вычислимые аналоги рекурсивно перечислимых множеств. В теории рекурсивных вычислений последние определялись двумя эквивалентными способами: как области значений общерекурсивных функций и как области определения частично рекурсивных функций. Но если оракул F не является всюду определенной функцией, то область определения F-вычислимой функции не обязана совпадать с областью значений тотальной F-вычислимой функции. Такая ситуация имеет место, например, в случае гиперарифметического оракула. Более того, область значений тотальной одноместной гиперарифметической функции – множество, разрешимое с гиперарифметическим оракулом. Здесь для оракула F_O подобное утверждение не рассматривается, но F_O-перечислимые множества определяются следующим образом.

Определение 2. Множество M называется F_O-перечислимым, если M есть область определения некоторой F_O-вычислимой функции. F_O-код этой функции называется перечисляющим F_O-кодом множества M.

Легко доказывается, что каждое F_O-разрешимое множество является F_O-перечислимым и что класс F_O-перечислимых множеств замкнут относительно операции пересечения. Но при доказательстве аналогов других свойств рекурсивно перечислимых множеств классические методы становятся неприменимыми, и приходится применять так называемую счетную селекторную функцию $\mu(z)$ из следующего утверждения.

Теорема 4. Существует F_O-вычислимая функция $\mu(z)$, которая по перечисляющему F_O-коду непустого F_O-перечислимого множества дает некоторый элемент этого множества.

Доказательство использует парную селекторную функцию из леммы 2, и аналогично [2, с. 51].

Теперь с помощью счетной селекторной функции $\mu(z)$ доказываются следующие свойства F_O-перечислимых множеств, аналогичные свойствам гиперарифметических множеств.

Теорема 5. 1. Класс F_O-перечислимых множеств замкнут относительно операций объединения и проецирования равномерно по перечисляющим F_O-кодам соответствующих множеств.

2. Если множество M и его дополнение $\overline{M}$ F_O-перечислимы, то M F_O-разрешимо равномерно по перечисляющим F_O-кодам M и $\overline{M}$.

3. Если график числовой функции $f(x)$ есть F_O-перечислимое множество, то $f(x)$ является F_O-вычислимой равномерно по перечисляющему F_O-коду ее графика.

Доказательство аналогично [2, с. 50].

Из леммы 3 следует, что каждое F_O-перечислимое множество является арифметическим, но обратное утверждение не выполняется. Для доказательства последнего факта вводятся следующие понятия. Пусть записи $B(F_O)$, $\overline{B}(F_O)$ *и* $\overline{\overline{B}}(F_O)$ обозначают множества инициальных машин $\langle z, x\rangle$, которые, работая с оракулом F_O без ограничения на диалог, удовлетворяют соответственно случаям 1–3, описанным в начале пункта 1. Эти множества также являются арифметическими, и, более того, первые два из них – F_O-перечислимые.

Теорема 6. Арифметическое множество $\overline{\overline{B}}(F_O)$ не является F_O-перечислимым.

Доказательство. От противного предполагается, что множество $\overline{\overline{B}}(F_O)$ – F_O-перечислимое, и пусть p_1, p_2 – перечисляющие F_O-коды множеств $\overline{B}(F_O)$, $\overline{\overline{B}}(F_O)$ соответственно. Вводится следующая процедура: для $<z, x>$ строится пара инициальных машин: $w_1 =< p_1, < z, x >>$ и $w_2 =< p_2, < z, x >>$. Затем задается вопрос $3^{<w_1, w_2>}$. Если ответ вида $< n, w_1 >$, то задается вопрос $2^{<z, x>}$ и полученный ответ 0 или 1 выдается в качестве результата данной процедуры. Если ответ вида $< n, w_2 >$, то сразу выдается результат 1. Доказывается, что эта процедура с оракулом F_O задает вычисление (без ограничения на диалог) следующей функции:

$$h(z, x) = \begin{cases} 0, \text{ } если \quad < z, x > \in B(F_O), \\ 1, \text{ } если \quad < z, x > \in \overline{B}(F_O) \cup \overline{\overline{B}}(F_O), \end{cases}$$

в остальных случаях значения $h(z, x)$ произвольные.

По определению, это означает, что оракул F_O является преднормальным в смысле [2, с. 37]. Тогда, согласно лемме 4 из [2, с. 47], любая гиперарифметическая функция является F_O-вычислимой, что противоречит теореме 3. Теорема доказана.

Таким образом, как и в случае рекурсивности, полная проблема остановки для вычислений с ограничением на диалог не является разрешимой ни с каким оракулом. Тогда строится оракул F_O, подобный гиперарифметическому оракулу, который решает проблему остановки для машин, хорошо работающих с ним же. Для F_O-вычислимых функций сохраняются основные принципы программирования и выполняются аналоги многих свойств гиперарифметических функций.

С другой стороны, классы F_O-разрешимых и F_O-перечислимых множеств содержатся в классе арифметических множеств.

Библиографический список

1. Ганов, В.А. Ограниченные вычисления с оракулами / В.А. Ганов, В.Р. Карымов // Известия АлтГУ. – 2009. – №1(61).

2. Ганов, В.А. Общая теория вычислений с оракулами / В.А. Ганов, Н.В. Белякин. – Новосибирск, 1989.

3. Роджерс, Х. Теория рекурсивных функций и эффективная вычислимость / Х. Роджерс. – М., 1973.