

УДК 510.5

Б. Я. Солон, Е. В. Ерёмкина

СТРУКТУРА Е-СТЕПЕНЕЙ ПЕРЕЧИСЛЕНИЙ
МНОЖЕСТВ НАТУРАЛЬНЫХ ЧИСЕЛ

В статье уточняется понятие перечисления множества натуральных чисел с использованием одного из фундаментальных понятий теории вычислимости — понятия сводимости по перечислимости. С помощью формализации понятия алгоритма в терминах машины Тьюринга и нашей формализации перечислений в статье приводятся эквивалентные определения сводимости по перечислимости.

Ключевые слова: сводимость по перечислимости, е-степень.

The article clarifies the notion of enumeration of the natural number set using one of the fundamental concepts of the computability theory — the concept of enumeration reducibility. With the formalization of the notion of algorithm in terms of Turing machines and the formalization of enumeration, the article gives an equivalent definition of enumeration reducibility.

Key words: enumeration reducibility, e-degree.

Пусть $\omega = \{0, 1, \dots\}$ — множество натуральных чисел. Будем использовать обозначения и термины, введенные в монографии [2]. Приведем те из них, которые будут использованы в нашей статье. Пусть $\{W_n : n \in \omega\}$ и $\{\varphi_n : n \in \omega\}$ — гёделева нумерация всех вычислимо перечислимых (в.п.) множеств и частично вычисляемых (ч.в.) функций. Обозначим через W_n^s , $s = 0, 1, 2, \dots$, конечную часть в.п. множества W_n , полученную после s -го шага работы ЭВМ перечисления множества W_n . Как обычно, D_u — конечное множество с каноническим индексом u , $\langle k, l \rangle$ — канторовский номер упорядоченной пары (k, l) . Если $t = \langle k, l \rangle$, то $\langle t \rangle_1 = k$ и $\langle t \rangle_2 = l$.

Для множества A будем обозначать

$$\begin{aligned} \langle A \rangle_1 &= \{x : \exists y[\langle x, y \rangle \in A]\}, \\ \langle A \rangle_2 &= \{y : \exists x[\langle x, y \rangle \in A]\}. \end{aligned}$$

Через $|A|$ будем обозначать мощность множества A и писать $|A| = \infty$, если A — бесконечное, и $|A| < \infty$, если A — конечное множество.

Для функции $\alpha : \omega \rightarrow \omega$ через $\delta\alpha$ будем обозначать область определения, через $\rho\alpha$ — область значений и через

$$\tau\alpha = \{\langle x, \alpha(x) \rangle : x \in \delta\alpha\}$$

— график функции α . Если $x \in \delta\alpha$, то будем писать также $\alpha(x)\downarrow$ и, если $x \notin \delta\alpha$, то — $\alpha(x)\uparrow$. Множество A называется *однозначным*, если $A = \tau\alpha$ для некоторой функции α . отождествим произвольное *перечисление множества* $A \neq \emptyset$ с некоторой тотальной функцией $p : \omega \rightarrow A$, область значений которой $\rho\alpha = A$. Пусть $P(A)$ — множество перечислений непустого множества A . Буквы f, g, p, q будем использовать только для обозначения *тотальных функций*. Последовательность $\langle 0, g(0) \rangle, \langle 1, g(1) \rangle, \dots$ бу-

дем называть перечислением tg в естественном порядке. Обозначим для множества A через

$$c_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \notin A, \end{cases} \quad \text{и} \quad \chi_A(x) = \begin{cases} 0, & \text{если } x \in A, \\ \uparrow, & \text{если } x \notin A, \end{cases}$$

характеристическую и частичную характеристическую функции множества A , соответственно.

Важное место в теории вычислимости занимает изучение вычислимо перечислимых (в.п.) множеств, по сути, теория вычислимости возникла в процессе формирования этого понятия. Интуитивно, в.п. множество — это такое множество натуральных чисел, элементы которого можно перечислить с помощью некоторого алгоритмического процесса. Этот алгоритмический процесс можно представить в виде работы ЭВМ перечисления (будем расшифровывать эту аббревиатуру как «Эффективная вычислительная машина»), которая производит вычисления по заданным инструкциям (или по программе) и которая имеет только *выход*. Работа ЭВМ происходит дискретно, шаг за шагом, причем на каждом шаге может появиться некоторое число на выходе, но может и не появиться. Те числа, которые появляются на выходе ЭВМ, и образуют некоторое в.п. множество.

Важность понятий в.п. множества и его неформального аналога ЭВМ перечисления обусловлена следующими причинами. Во-первых, формальное описание алгоритмически вычислимых функций невозможно без рассмотрения частично вычислимых функций и их областей определения (последние и есть в.п. множества). Во-вторых, многие известные неразрешимые проблемы (такие как, например, проблема равенства слов в ассоциативном исчислении, проблема разрешимости исчисления предикатов, 10-я проблема Гильберта и т. д.), формализованные в арифметике, сводятся к проблеме вычислимости того или иного в.п. множества.

Тем не менее, класс в.п. множеств не может охватить весь класс множеств натуральных чисел и, следовательно, весь класс неразрешимых проблем. Поэтому зачастую приходится исследовать возможность эффективного перечисления множества A , которое может не быть вычислимо перечислимым, с использованием *известного* перечисления другого множества B . Если это так, то мы говорим, что множество A *сводится по перечислимости* (или, как говорят для краткости, *e-сводится*) к множеству B (обозначение: $A \leq_e B$).

Уточним это интуитивное определение относительной перечислимости, используя понятие ЭВМ перечисления. Пусть даны множества A и B . ЭВМ перечисления, описанную выше, несколько модернизируем, снабдив её *входом*. Работа ЭВМ происходит, как и ранее, по заданной программе и время от времени появляется некоторое число на выходе, однако в ней предусмотрено, что время от времени требуется «входное» число. Если затребован вход, то может быть подано любое натуральное число или не подано никакого числа. Пусть на вход подаются элементы множества B , а на выходе появляются элементы множества A . Порядок, в котором появляются элементы множества A , может меняться при изменении порядка подачи элементов B на вход. Будем допускать также повторяемость элементов в пересчете множества B и в пересчете множества A . Тогда множество A *алгоритмически перечислимо относительно B* или A *сводится*

по перечислимости к B , если существует ЭВМ перечисления, которая, получая в качестве входов элементы B в каком бы то ни было порядке, на выходе перечисляет множество A в некотором порядке.

Если сформулировать это определение кратко, то скажем, что A сводимо по перечислимости или e -сводимо (от английского аналога *enumeration reducibility*) к множеству B , если существует ЭВМ перечисления A из любого перечисления множества B .

Приведем формальное определение этого интуитивно заданного понятия, принадлежащее Роджерсу и Фридбергу [2].

Определение. $A \leq_e B \Leftrightarrow \exists n \forall x [x \in A \Leftrightarrow \exists u [(x, u) \in W_n \ \& \ D_u \subseteq B]]$.

Пусть, как обычно,

$$A \equiv_e B \Leftrightarrow A \leq_e B \ \& \ B \leq_e A, \\ \text{deg}_e(A) = \{X : X \equiv_e A\}$$

— e -степень множества A (для обозначения e -степеней будем также использовать малые жирные латинские буквы, например, $\mathbf{a} = \text{deg}_e(A)$). Отношение \leq_e на 2^ω индуцирует частичный порядок \leq на множестве e -степеней:

$$\text{deg}_e(A) \leq \text{deg}_e(B) \Leftrightarrow A \leq_e B.$$

Обозначим через D_e множество e -степеней, упорядоченное отношением \leq , и через $D_e(<\mathbf{a}) = \{\mathbf{x} : \mathbf{x} < \mathbf{a}\}$.

Непосредственно из определения e -сводимости, как интуитивного, так и формального, следует, что все в.п. множества e -эквивалентны и образуют наименьшую в D_e e -степень. Кроме того, известно, что D_e — верхняя полурешетка, не решетка с наименьшим элементом.

e -степени, содержащие графики тотальных функций, называются *тотальными*. Обозначим через T множество тотальных e -степеней, частично упорядоченное отношением \leq . Обозначения $T(<\mathbf{a})$ и $T(\leq\mathbf{a})$ используются в обычном смысле.

Предложение 1. e -степень $\mathbf{a} = \text{deg}_e(A)$ тотальна тогда и только тогда, когда $A \equiv_e p$ для некоторого перечисления $p \in P(A)$.

Предложение 2. T — верхняя подполурешетка D_e .

Предложения 1 и 2 были доказано в статье [4].

Термин *нетотальная e -степень* применим, таким образом, к e -степеням, которые не содержат графиков ни одной тотальной функции, то есть к элементам множества $D_e \setminus T$. Первый серьезный результат о e -сводимости был получен Ю. Т. Медведевым [1], а именно, было доказано, что существуют нетотальные e -степени, то есть, что $D_e \setminus T \neq \emptyset$.

Так как $\tau_{cA} \in \text{deg}_T(A)$ для любого множества A , то при изучении T -степеней можно идентифицировать множество A его характеристической функцией c_A . Для e -степеней эта ситуация невозможна. Ясно, что любая нетотальная e -степень не содержит никаких характеристических функций. Не столь очевидно, что тотальные e -степени не содержат графики характеристических функций некоторых множеств, принадлежащих им. Другими словами, можно доказать (и это сделано в [3]), что для любой функции f существует множество A такое, что $A \equiv_e f$ и $c_A \not\equiv_e f$, то есть

$\tau c_A \notin \deg_e(f)$. В то же время, как легко заметить, $\deg_e(A)$ содержит $\tau\chi_A$ для любого множества A .

Обозначим через $D_e(A)$ частично упорядоченное (отношением \leq на D_e) множество e -степеней, содержащих некоторое перечисление множества A :

$$D_e(A) = \{\deg_e(\tau p) : p \in P(A)\}.$$

Легко проверить, что $D_e(A)$ — верхняя подполурешетка D_e и $D_e(A) \subseteq T$ для любого множества A . Нас интересуют свойства $D_e(A)$ для различных множеств A . Заметим, что если $|A| = 1$, то $D_e(A) = \{0_e\}$.

В статье [4] доказана следующая теорема 1, полностью описывающая $D_e(A)$ в случае, когда A — в.п. множество и $|A| \geq 2$.

Теорема 1. *Если A — вычислимо перечислимое множество и $|A| \geq 2$, то $D_e(A) = T$ и верхние полурешетки $D_e(A)$ и T изоморфны.*

Другая ситуация — в случае, когда A не является в.п. множеством. В статье [4] доказана следующая

Теорема 2. *Если множество A не является вычислимо перечислимым, то $D_e(A) \subset T \setminus \{0_e\}$, то есть не любая тотальная e -степень содержит перечисление множества A .*

В то же время, имеет место

Теорема 3. *Если $|A| \geq 2$ и $a = \deg_e(A)$, то $T(\geq a) = D_e(A)$ и частично упорядоченные множества $T(\geq a)$ и $D_e(A)$ изоморфны.*

Доказательство. Пусть $a_0 \neq a_1$ — элементы множества A . Докажем сначала, что $T(\geq a) \subseteq D_e(A)$.

Пусть тотальная e -степень $g = \deg_e(\tau g) \in T(\geq a)$, тогда $A = \Phi_z(\tau g)$ для некоторого z . Рассмотрим функцию f , заданную рекурсивной схемой:

$$f(0) = \begin{cases} \min \Phi_z^0(\tau g), & \text{если } \Phi_z^0(\tau g) \neq \emptyset, \\ a_0, & \text{если } \Phi_z^0(\tau g) = \emptyset, \end{cases} \quad \text{и}$$

$$f(n+1) = \begin{cases} \min(\Phi_z^{n+1}(\tau g) - \{f(n)\}), & \text{если } \Phi_z^{n+1}(\tau g) - \{f(n)\} \neq \emptyset, \\ f(n), & \text{если } \Phi_z^{n+1}(\tau g) - \{f(n)\} = \emptyset. \end{cases}$$

Так как $A = \Phi_z(\tau g)$, то $f \leq_e g$ и $\rho f = A$. Определим перечисление $p \in P(A)$ следующим образом:

$$p(x) = \begin{cases} f(y), & \text{если } x = 2y, \\ a_0, & \text{если } x = 2y + 1 \ \& \ y \in \tau g, \\ a_1, & \text{если } x = 2y + 1 \ \& \ y \notin \tau g. \end{cases}$$

Ясно, что $p \in P(A)$ и $p \equiv_e g$, откуда следует, что $g \in D_e(A)$.

Проверим теперь, что $D_e(A) \subseteq T(\geq a)$. Так как $A \leq_e p$, то для любой e -степени b имеем

$$b \in D_e(A) \Rightarrow (\exists p \in P(A))[p \in b] \Rightarrow A \leq_e p \Rightarrow a \leq b \Rightarrow b \in T(\geq a),$$

следовательно, $D_e(A) \subseteq T(\geq a)$.

Теперь докажем изоморфизм частично упорядоченных множеств $D_e(A)$ и $T(\geq a)$. Пусть $\iota: D_e(A) \rightarrow T(\geq a)$, $\iota(\deg_e(\tau p)) = \deg_e(\tau p)$, то есть ι — тождественное инъективное отображение. Для любой тотальной функ-

ции f , если $A \leq_e f$, то существует перечисление $p \in P(A)$ такое, что $p \equiv_e f$, поэтому ι — сюръективное отображение. Следовательно, частично упорядоченные множества $D_e(A)$ и $T(\geq a)$ изоморфны и теорема доказана.

Прежде чем доказать основную теорему, рассмотрим еще один подход к е-сводимости, позволяющий расширить интуитивную базу этого понятия. Сначала дадим ряд определений.

Обозначим

$$\Phi_n^s(X) = \{x : \exists u[\langle x, u \rangle \in W_n^s \ \& \ D_u \subseteq X]\}.$$

Очевидно, $\Phi_n^s(X)$ — конечное множество и $\Phi_n^s(X) \subseteq \Phi_n^{s+1}(X)$ для всех $n, s \in \omega$. Кроме того,

$$A = \Phi_n(B) \Rightarrow A = \bigcup_{s \in \omega} \Phi_n^s(B).$$

Последовательность $\{B^s : s \in \omega\}$ называется *конечной аппроксимацией* множества B , если $|B^s| < \infty$, $B^s \subseteq B^{s+1} \subseteq B$ для всех $s \in \omega$ и $B = \bigcup_{s \in \omega} B^s$. Пусть $A = \Phi_n(B)$, опишем *перечисление* A , связанное с данной конечной аппроксимацией множества B и e -оператором Φ_n . Пусть $\Phi_n^{s_0}(B^{s_0})$ — первое непустое множество, расположим его элементы в некотором фиксированном порядке (например, в порядке возрастания): a_0, \dots, a_{n_0} . Для всех $s \geq s_0$ элементы $\Phi_n^s(B^s)$ будем располагать в некотором фиксированном порядке (например, в порядке возрастания) и последовательно добавлять к полученному ранее начальному отрезку перечисления множества A . Например, элементы множества $\Phi_n^{s_0+1}(B^{s_0+1})$ получат номера $a_{n_0+1}, \dots, a_{n_1}$, и т. д. В результате получим перечисление $p: \omega \rightarrow A$ множества A такое, что $p(n) = a_n$ для всех $n \in \omega$. Перечисление множества A зависит от выбора конечной аппроксимации $\{B^s : s \in \omega\}$ множества B .

Будем называть W -оператором любое отображение

$$F: 2^\omega \rightarrow 2^\omega,$$

$$F(X) = \bigcup_{s \in \omega} F^s(X^s),$$

где

$$F^s(X) = \{x : \exists u[\langle x, u \rangle \in W^s \ \& \ D_u \subseteq X]\},$$

$\{W_s : s \in \omega\}$ — фиксированная конечная аппроксимация множества W и $\{X^s : s \in \omega\}$ — произвольная конечная аппроксимация множества X . Заметим, что, вообще говоря, W -оператор не является однозначным отображением и $F(X)$ зависит от выбранной аппроксимации $\{X^s : s \in \omega\}$.

Будем называть W -оператор B -униформным, если $F(B)$ — одно и то же множество, не зависящее от конечной аппроксимации $\{B^s : s \in \omega\}$ множества B . В случае B -униформного W -оператора F имеем

$$F(B) = \bigcup_{s \in \omega} F^s(B).$$

Наконец, скажем, что W -оператор *униформен*, если он B -униформный для любого множества B .

Если W — в.п. множество и $\{W^s : s \in \omega\}$ — вычислимая конечная аппроксимация множества W , то W -оператор, будем называть *по-*

что e -оператором. Легко заметить, что в нашей терминологии любой e -оператор — это равномерный почти e -оператор.

Определим сводимость множеств, которая на первый взгляд «шире» e -сводимости: множество A *интуитивно e -сводимо* к множеству B (обозначение: $A \leq_{ie} B$), если существует B -униформный почти e -оператор F такой, что $A = F(B)$. Очевидно, что если $A \leq_e B$, то $A \leq_{ie} B$. Оказывается, верна и обратная импликация.

Теорема 4. Для любых множеств A и B $A \leq_{ie} B \Leftrightarrow A \leq_e B$.

Следующая теорема 5 имеет интуитивную подоплеку. Как оказалось, e -сводимость множеств можно эквивалентным образом определить через перечисления (рассматриваемые как тотальные функции), причем в этом определении можно переставить кванторы (см. для сравнения интуитивное определение e -сводимости): множество A e -сводится к множеству B , если для **любого** перечисления B **существует** алгоритм, позволяющий получить некоторое перечисление A . Формально, имеет место следующая

Теорема 5. $A \leq_e B \Leftrightarrow (\forall p \in \mathbf{P}(B))(\exists n)[A = \Phi_n(\tau p)]$.

Доказательство. Пусть $A \leq_e B$, тогда $A = \Phi_l(B)$ для некоторого l . Так как $B \leq_e \tau p$ для любого перечисления $p \in \mathbf{P}(B)$, то $B = \Phi_m(\tau p)$ для некоторого m (зависящего, вообще говоря, от p). Рассмотрим оператор $\Psi(X) = \Phi_l(\Phi_m(X))$. Ясно, что Ψ — e -оператор и $\Psi = \Phi_n$ для некоторого n . Мы имеем, таким образом,

$$A = \Phi_l(B) = \Phi_l(\Phi_m(\tau p)) = \Phi_n(\tau p),$$

что и требовалось доказать.

Обратно, пусть

$$(\forall p \in \mathbf{P}(B))(\exists n)[A = \Phi_n(\tau p)].$$

Ясно, что в этом случае $A \leq_e \tau p$ для любого перечисления $p \in \mathbf{P}(B)$.

Если $|B| < \infty$, то A — вычислимо перечислимое множество и тогда теорема выполнена тривиально. Пусть B — бесконечное множество, $B = \{b_0, b_1, \dots\}$ и $b_0 < b_1$. Обозначим

$$\mathbf{P}_n(B) = \{f : f \in \mathbf{P}(B) \ \& \ A = \Phi_n(\tau f)\}.$$

Будем использовать далее буквы α и β в качестве переменных для начальных сегментов перечислений B . Для завершения доказательства теоремы нам понадобится следующая

Лемма. $(\exists n)(\exists \alpha)(\forall \beta)[\alpha \subseteq \beta \rightarrow (\exists f \in \mathbf{P}_n(B))[\beta \subseteq f]]$.

Доказательство леммы. Допустим, что утверждение леммы неверно и

$$(\forall n)(\forall \alpha)(\exists \beta)[\alpha \subseteq \beta \ \& \ (\forall f \in \mathbf{P}_n(B))[\beta \not\subseteq f]].$$

Это, в частности, означает, что

$$(\forall n)(\forall \alpha)(\exists \beta)[\alpha \subseteq \beta \ \& \ (\forall f \in \mathbf{P}_n(B))[\beta \subseteq f \rightarrow f \notin \mathbf{P}_n(B)]]. \quad (1)$$

Построим последовательность конечных функций $\{\gamma_i : i \in \omega\}$ такую, что $\gamma_i \subseteq \gamma_{i+1}$ и $\rho \gamma_i \subseteq B$ для всех $i \in \omega$. Полагаем $\gamma_0 = \emptyset$. Пусть γ_n уже построена. Для данных n и $\alpha = \gamma_n$ пусть β^* — конечная функция, для ко-

торой $\tau\beta$ имеет наименьший канонический индекс среди β , удовлетворяющих условию (1). Полагаем

$$\tau\gamma_{n+1} = \tau\beta^* \cup \{ \langle x_n, b_n \rangle \}.$$

Очевидно, что $\gamma_i \subseteq \gamma_{i+1}$ и $\rho\gamma_i \subseteq B$ для всех $i \in \omega$.

Пусть

$$f = \bigcup_{i \in \omega} \gamma_i.$$

Из построения видно, что f — тотальная функция. Так как $b_n \in \rho\gamma_{n+1}$ для всех n , то $\rho f = B$, поэтому $f \in \mathbf{P}(B)$ и, следовательно, $A \leq_e \tau f$. Пусть $f \in \mathbf{P}_n(B)$, то есть $A = \Phi_n(\tau f)$. Однако, так как (найденная по данному n) функция $\beta^* \subseteq f$ в силу (1), это влечет, что $f \notin \mathbf{P}_n(B)$. Полученное противоречие доказывает лемму.

Пусть n^* — наименьшее число и α^* — конечная функция, для которой $\tau\alpha^*$ имеет наименьший канонический индекс среди n и α , удовлетворяющих доказанной выше лемме. Рассмотрим множество

$$V = \{ \langle x, v \rangle : D_v = \langle D_u \rangle_2 \ \& \ \langle x, u \rangle \in W_{n^*} \ \& \\ \& \ \tau\alpha^* \cup D_u \text{ — однозначное множество} \}.$$

Ясно, что V — в.п. множество и $V = W_m$ для некоторого m . Покажем, что в этом случае $A = \Phi_m(B)$, и тогда теорема будет полностью доказана.

Пусть $x \in A$ и $f \in \mathbf{P}_{n^*}(B)$ — такая функция, что $\alpha^* \subseteq a$. Так как $A = \Phi_{n^*}(\tau f)$, то

$$\langle x, u \rangle \in W_{n^*} \ \& \ D_u \subseteq \tau f$$

для некоторого u . Так как $D_u \subseteq \tau f$ и $\tau\alpha^* \subseteq \tau f$, то $D_u \cup \tau\alpha^*$ — однозначное множество, $\langle x, v \rangle \in W_m$, где $D_v = \langle D_u \rangle_2$, и $D_v \subseteq \rho f = B$. Следовательно, $x \in \Phi_m(B)$ и $A \subseteq \Phi_m(B)$.

Докажем обратное включение. Пусть $x \in \Phi_m(B)$, то есть

$$(\exists u)[\langle x, u \rangle \in W_{n^*} \ \& \ \tau\alpha^* \cup D_u \in SV \ \& \ D_v \subseteq B].$$

Пусть $\tau\beta = \tau\alpha^* \cup D_u$. Очевидно, $\tau\alpha^* \subseteq \tau\beta$ и $\rho\beta \subseteq B$, поэтому, в силу леммы, найдется такая функция $f \in \mathbf{P}_n(B)$, что $\beta \subseteq f$. Так как $\langle x, u \rangle \in W_{n^*}$ и $D_u \subseteq \tau\beta \subseteq \tau f$, то $x \in \Phi_{n^*}(\tau f) = A$, то есть $\Phi_m(B) \subseteq A$. Теорема доказана.

Библиографический список

1. Медведев Ю. Т. Степени трудности массовых проблем // Доклады АН СССР. 1955. Т. 104, № 4. С. 501–594.
2. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972. 624 с.
3. Солон Б. Я. Соотношения между ϵ -степенями и Т-степенями // Известия высших учебных заведений. Математика. 1995. Т. 394, № 3. С. 51–61.
4. Солон Б. Я., Ерёмкина Е. В. Перечисления множеств и степени перечислимости // Евразийский Союз Ученых. Ежемесячный научный журнал. 2014. № 8. С. 17–20.