Зимний коллоквиум по дискретной математике 2019

hse-ami-open-exams

Содержание

1 Определение вычислимой частичной функции из $\mathbb{N}$ в $\mathbb{N}$. Счетность семейства частичных вычислимых функций, и существование невычислимых функций. Разрешимость подмножества $\mathbb{N}$. Перечислимые подмножества $\mathbb{N}$. Счетность семейства перечислимых множеств, и существование неперечислимых множеств.

1.1 Определение вычислимой частичной функции из $\mathbb{N}$ в $\mathbb{N}$

Определение 1. *Пусть A и B некоторые множества. Частичной функцией из A в B называется произвольное подмножество $f \subseteq A \times B$, удовлетворяющая свойству*

$$\forall a \in A, b_1, b_2 \in B \, (a, b_1) \in f \wedge (a, b_2) \in f \Rightarrow b_1 = b_2$$

Обозначение: $f : A \xrightarrow{p} B$

Определение 2. *Функция $f : A \xrightarrow{p} B$ вычислима, если существует программа (на C, на ассемблере, машина Тьюринга и т.п.), которая на любом входе $x \in \operatorname{dom} f$ выписывает $f(x)$ и завершается, а на любом входе $x \in A \setminus \operatorname{dom} f$ не завершается ни за какое конечное число шагов.*

1.2 Счетность семейств частичных вычислимых функций, и существование невычислимых функций.

Утверждение 1. *Множество частичных вычислимых функций не более, чем счетно.*

Доказательство. Действительно, всякой вычислимой функции можно поставить в соответствие алгоритм, причем различные функции вычисляются различными алгоритмами. Алгоритм – это конечная строка. То есть множество алгоритмов счетно. Существует инъекция из множества вычислимых функций в множество алгоритмов, следовательно, множество вычислимых функций не более, чем счетно. ☐

Утверждение 2. *Существуют невычислимые функции $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$.*

Доказательство. Множество всех функций из $\mathbb{N}$ в $\mathbb{N}$ имеет мощность континуум, а множество вычислимых функций не более, чем счетно. Следовательно, множество невычислимых функций не пусто. ☐

1.3 Разрешимость подмножества $\mathbb{N}$.

Определение 3. *Множество A разрешимо, если его характеристическая функция*

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

вычислима.

1.4 Перечислимые подмножества $\mathbb{N}$.

Определение 4. *Множество A пречислимо, если есть программа, на пустом входе последовательно выписывающая все элементы A и только их.*

1.5 Счетность семейства перечислимых множеств, и существование неперечислимых множеств.

Утверждение 3. *Множество перечислимых множеств* $\mathbb{N}$ *не более, чем счетно.*

Доказательство. Всякому перечислимому множеству соответствует алгоритм, который его перечисляет, причем разные множества перечисляются разными алгоритмами. Отсюда следует, что мощность множества перечислимых множеств $\mathbb{N}$ не превосходит мощность множества алгоритмов, которое является счетным. $\square$

Утверждение 4. *Существуют неперечислимые множества* $A \subseteq \mathbb{N}$.

Доказательство. Множество перечислимых множеств не более, чем счетно. А множество всех подмножеств $\mathbb{N}$ имеет мощность континуум. Следовательно, множество неперечислимых подмножеств $\mathbb{N}$ не пусто. $\square$

2 Эквивалентные определения перечислимости (полуразрешимость, область определения вычислимой функции, множество значений вычислимой функции).

Определение 5. *Множество A полуразрешимо, если его полухарактеристическая функция*

$$w_A(x) = \begin{cases} 1, & \text{если}\, x \in A \\ \text{не определено}, & \text{если}\, x \notin A \end{cases}$$

вычислима.

Пусть $f : A \xrightarrow{p} B$.

Определение 6. *Область определения f*

$$\operatorname{Dom} f = \{a \in A \mid \exists b \in B\ (a, b) \in f\}$$

Определение 7. *Область значений f*

$$\operatorname{Ran} f = \{b \in B \mid \exists a \in A\ (a, b) \in f\}$$

Утверждение 5. *Следующие утверждения эквивалентны:*

1. *Множество A перечислимо.*
2. *Множество A полуразрешимо.*
3. $\exists f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, *$f$ вычислимая, т.ч.* $\operatorname{Dom} f = A$.
4. $\exists f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, *$f$ вычислимая, т.ч.* $\operatorname{Ran} f = A$.

Доказательство. 1) $\Rightarrow$ 2)
Опишем алгоритм, вычисляющий $w_A(x)$: запускаем перечислитель A, если на каком-то шаге встретился x, то вернем 1. Так как перечислитель печатает все элементы A и только их, то если $x \in A$, то на каком-то шаге он напечатает его и алгоритм вернет 1, а если же $x \notin A$, то алгоритм не закончится ни за какое конечное кол-во шагов.

2) $\Rightarrow$ 3)
$f = w_A$. Действительно, знаем, что w_A вычислима и $\operatorname{Dom} w_A = A$.

3) $\Rightarrow$ 4)
Пусть есть вычислимая функция $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$. Определим функцию g:

$$g(x) = \begin{cases} x, & \text{если}\, x \in \operatorname{Dom} f \\ \text{не определено}, & \text{иначе} \end{cases}$$

Функция g вычислима (т.к. f вычислима), более того $\operatorname{Ran} g = \operatorname{Dom} f$.

4) $\Rightarrow$ 1)
Так как f вычислимая, то существует алгоритм F, который вычисляет значение f. Опишем алгоритм перечислителя: на n-ой итерации запустим по очереди $\forall i \in \{0, 1, \ldots, n\}$ $F(i)$ на n шагов. Таким образом, $\forall x \in \operatorname{Ran} f$ алгоритм $F(x)$ будет запущен на необходимое кол-во шагов для того, что вычислить значение $f(x)$. Следовательно, множество $A = \operatorname{Ran} f$ перечислимо. □

3 Теорема Поста. Теорема о графике.

3.1 Теорема Поста

Теорема 1 (Теорема Поста)**.** *Множества A и $\overline{A}$ перечислимы тогда и только тогда, когда A разрешимо.*

Доказательство. $\Rightarrow$
Построим алгоритм, вычисляющий $\chi_A(x)$: будем по очереди делать по одному шагу для $w_A(x)$ и $w_{\overline{A}}(x)$, т.к. $x \in A \vee x \in \overline{A}$, то какой-то один из алгоритмов вернет 1 на каком-то шаге. Если это будет w_A, то вернем 1, если же $w_{\overline{A}}$, то вернем 0.
$\Leftarrow$
Очевидно, из разрешимости следует перечислимость. Если A разрешимо, то и $\overline{A}$ разрешимо. $\square$

3.2 Теорема о графике

Определение 8. *Пусть задана функция $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$. Графиком функции f называется множество $\Gamma_f = \{(x, f(x)) \mid x \in \operatorname{Dom} f\}$.*

Теорема 2 (Теорема о графике)**.** *Функция $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$ вычислима тогда и только тогда, когда ее график Γ_f перечислим.*

Доказательство. $\Rightarrow$
Пусть f вычислима. Тогда $\operatorname{Dom} f$ вычислима и, следовательно, есть вычислимая функция g, т.ч. $\operatorname{rng} g = \operatorname{Dom} f$. Рассмотрим функцию $h : \mathbb{N} \to \mathbb{N}^2$, т.ч. $h(x) \simeq (g(x), f(g(x)))$ для всех $x \in \mathbb{N}$. Она вычислима, причем

$$(x, y) \in \operatorname{rng} h \Leftrightarrow (x \in \operatorname{rng} g \wedge y = f(x)) \Leftrightarrow (x \in \operatorname{Dom} f \wedge y = f(x)) \Leftrightarrow (x, y) \in \Gamma_f$$

для всех $x, y \in \mathbb{N}$. Значит, $\Gamma_f = \operatorname{rng} h$, следовательно, Γ_f перечислим (т.к. h вычислимая).
$\Leftarrow$
Пусть Γ_f перечислим. Тогда, чтобы вычислить $f(x)$, достаточно выписывать элементы Γ_f и проверять, совпадает ли первая координата пары с x. Если совпадает, выдавать вторую координату. Этот процесс завершается тогда и только тогда, когда $x \in \operatorname{Dom} f$. $\square$

4 Универсальные вычислимые функции (нумерации) для семейства частичных вычислимых функций натурального аргумента. Несуществование универсальной вычислимой функции для семейства тотальных вычислимых функций натурального аргумента (диагональное рассуждение). Главные универсальные функции.

4.1 Универсальные вычислимые функции (нумерации) для семейства частичных вычислимых функций натурального элемента.

Определение 9. *Функций $U : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ называется универсальной вычислимой, если она вычислима и для всякой вычислимой функции $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$ найдется такое число $n \in \mathbb{N}$, называемое индексом функции f относительно U, т.ч. $U_n = f$, т.е.*

$$\forall x(f(x) \simeq U(n, x))$$

4.2 Несуществование универсальной вычислимой функции для семейства тотальных вычислимых функций натурального аргумента (диагональное рассуждение).

Утверждение 6. *Не существует универсальной функции для семейства тотальных вычислимых функций.*

Доказательство. Допустим, что это не так и существует такая функция U. Тогда функция

$$f(x) = U(x, x) + 1$$

является тотальной и вычислимой. Следовательно, найдется такое $n \in \mathbb{N}$, что $f(x) = U(n, x)$. Так как f тотальна, то можем подставить n вместо x:

$$U(n, n) = f(n) = U(n, n) + 1$$

Противоречие. Следовательно, такой функции не существует. □

4.3 Главные универсальные функции.

Определение 10. *Вычислимая функция $U : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ называется главной универсальной вычислимой функцией, если для любой вычислимой функции $V : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ найдется вычислимая тотальная функция $s : \mathbb{N} \to \mathbb{N}$, т.ч. $V_n = U_{s(n)}$ для всех $n \in \mathbb{N}$, т.е.*

$$\forall x \forall n V_n(x) \simeq U(s(n), x)$$

5 Вычислимая функция, не имеющая тотального вычислимого продолжения. Перечислимое неразрешимое множество. Неразрешимость проблемы применимости.

5.1 Вычислимая функция, не имеющая тотального вычислимого продолжения.

Определение 11. *Функция g является продолжением функции f, если* $\operatorname{Dom} f \subset \operatorname{Dom} g$ *и* $\forall x \in \operatorname{Dom} f\ g(x) = f(x)$.

Утверждение 7. *Существует вычислимая функция, не имеющая вычислимого тотального продолжения.*

Доказательство. Пусть $d(x) \simeq U(x,x)$, d вычислима. Предположим, что вычислимая тотальная функция g продолжает d. Тогда функция h, т.ч. $h(x) = g(x)+1$ для всех $x \in \mathbb{N}$, также будет вычислимой тотальной. Пусть $h = U_n$, h определена всюду, значит $n \in \operatorname{Dom} d$. Тогда $U_n(n) = h(n) = g(n)+1 = d(n)+1 = U_n(n)+1$, что неверно. Следовательно, вычислимого тотального продолжения функции d не существует. □

5.2 Перечислимое неразрешимое множество.

Утверждение 8. *Множество $K := \{n \mid U_n(n)$ определено$\}$ перечислимо, но не разрешимо.*

Доказательство. Перечислимость очевидна, поскольку $K = \operatorname{Dom} d$, где вычислимая функция $d : \mathbb{N} \xrightarrow{p} \mathbb{N}$ такова, что $d(x) \simeq U(x,x)$ для всех $x \in \mathbb{N}$.
Установим неразрешимость K. Предположим противное. Тогда функция

$$g(x) = \begin{cases} d(x), & x \in \operatorname{Dom} d \\ 0, & x \notin \operatorname{Dom} d \end{cases}$$

является тотальной, более того вычислимой (поскольку $d(x)$ вычислима и $\operatorname{Dom} d$ разрешимо). Но мы знаем, что d не имеет тотального вычислимого продолжения. Противоречие. Следовательно, K неразрешимо. □

5.3 Неразрешимость проблемы применимости (остановки).

Определение 12. *Задача разрешения множества $S := \{(n,x) | U(n,x)$ определено$\}$ называется проблемой применимости (остановки).*

Теорема 3. *Проблема применимости (остановки) неразрешима.*

Доказательство. Пусть χ_S вычисляется алгоритмом S. Тогда, запустив $S(x,x)$, можно разрешить множество $\{x \mid U_x(x)$ *определено*$\}$, для которого доказана неразрешимость. □

6 Теорема Поста. Существование перечислимого множества, дополнение которого неперечислимо. Перечислимые неотделимые множества.

6.1 Теорема Поста

Теорема 4 (Теорема Поста)**.** *Множества A и $\overline{A}$ перечислимы тогда и только тогда, когда A разрешимо.*

Доказательство. $\Rightarrow$
Построим алгоритм, вычисляющий $\chi_A(x)$: будем по очереди делать по одному шагу для $w_A(x)$ и $w_{\overline{A}}(x)$, т.к. $x \in A \vee x \in \overline{A}$, то какой-то один из алгоритмов вернет 1 на каком-то шаге. Если это будет w_A, то вернем 1, если же $w_{\overline{A}}$, то вернем 0.
$\Leftarrow$
Очевидно, из разрешимости следует перечислимость. Если A разрешимо, то и $\overline{A}$ разрешимо. □

6.2 Существование перечислимого множества, дополнение которого неперечислимо.

Утверждение 9. *Существует перечислимое множество, дополнение которого перечислимо.*

Доказательство. Множество $K = \{x \mid U_x(x) \text{ *определено*}\}$ перечислимо, но не разрешимо. Тогда $\overline{K}$ неперечислимо. Если $\overline{K}$ было бы перечислимо, то по теореме Поста, оно было бы разрешимо. □

6.3 Перечислимые неотделимые множества.

Определение 13. *Множества A, B называются отделимыми, если существует множество C, т.ч. $A \subseteq C$ и $B \cap C = \emptyset$.*

Утверждение 10. *Существуют непересекающиеся перечислимые множества, которые нельзя отделить разрешимом множеством.*

Доказательство. Рассмотрим множества $A = \{x \mid U_x(x) = 42\}$, $B = \{x \mid U_x(x) = 0\}$. Они перечислимы и не пересекаются. Допустим, существует разрешимое C, отделяющее A и B. Пусть оно содержит в себе множество A. Тогда:

$$\chi_C(x) = \begin{cases} 1, & \text{если } U_x(x) = 42, \\ 0, & \text{если } U_x(x) = 0, \\ \text{и что-то ещё на других числах.} \end{cases}$$

χ_C вычислима. Значит, $\exists n \; \chi_C(x) = U_n(x)$ Но пусть тогда $x = n$. Получаем:

$$U_n(n) = \begin{cases} 1, & \text{если } U_n(n) = 42, \\ 0, & \text{если } U_n(n) = 0, \\ \text{и что-то ещё на других числах.} \end{cases}$$

Получили противоречие. □

7 Сводимости: m-сводимость и Тьюрингова сводимость. Их свойства. Полные перечислимые множества.

7.1 m-сводимость.

Определение 14. *Множество A **m-сводится** к множеству B, если существует тотальная вычислимая функция f такая, что $\forall x\ x \in A \iff f(x) \in B$. Обозначается как $A \leqslant_m B$.*

Свойства m-сводимости:

- $A \leqslant_m A$ (рефлексивность),
- $A \leqslant_m B \wedge B \leqslant_m C \implies A \leqslant_m C$ (транзитивность),
- $\left.\begin{array}{l} B \text{ разрешимо} \\ A \leqslant_m B \end{array}\right\} \implies A \text{ разрешимо},$
- $\left.\begin{array}{l} A \text{ неразрешимо} \\ A \leqslant_m B \end{array}\right\} \implies B \text{ неразрешимо}.$

7.2 Тьюрингова сводимость.

Определение 15. *Множество A **T-сводится** (сводится по Тьюрингу) к множеству B, если при помощи алгоритма вычисления χ_B (не обязательно существующего) можно вычислить χ_A. Обозначается как $A \leqslant_T B$.*

Свойства Тьюринговой сводимости:

- $A \leqslant_T A$ (рефлексивность),
- $A \leqslant_T B \wedge B \leqslant_T C \implies A \leqslant_T C$ (транзитивность),
- $\left.\begin{array}{l} B \text{ разрешимо} \\ A \leqslant_T B \end{array}\right\} \implies A \text{ разрешимо},$
- $\left.\begin{array}{l} A \text{ неразрешимо} \\ A \leqslant_T B \end{array}\right\} \implies B \text{ неразрешимо}.$
- $A \leqslant_m B \Rightarrow A \leqslant_T B$
- $A \leqslant_T \overline{A}$

Определение 16. *Перечислимое множество, к которому m-сводится любое другое перечислимое множество, называется **полным перечислимым множеством**.*

Теорема 5. *Существует полное перечислимое множество.*

Доказательство. Рассмотрим множество $A = \{(n, x) \mid U_n(x) \text{ определено}\}$. Заметим, что оно перечислимо. Пусть мы хотим свести некоторое перечислимое множество B к множеству A. Знаем, что в силу перечислимости существует вычислимая частичная функция f такая, что $B = \operatorname{Dom} f$. Эта функция должна присутствовать в универсальной нумерации. Пусть это U_n. Тогда для того, чтобы проверить принадлежность $x \in B$, достаточно проверить принадлежность $(n, x) \in A$. Сводящая функция в данном случае выглядит как $m(x) = (n, x)$. ☐

8 Теорема Клини о неподвижной точке.

Теорема 6. *Для всякой тотальной вычислимой функции f и главной нумерации U_n найдётся n такое, что $U_n = U_{f(n)}$.*

Доказательство. Педагогический трюк для лучшего запоминания: сначала попытаемся доказать ложное утверждение о том, что у всякой тотальной вычислимой функции есть неподвижная точка, то есть число n такое, что $n = f(n)$.
Функция f вычислима, функция $U_x(x)$ вычислима, значит, вычислима их композиция. То есть, существует m такое, что

$$f(U_x(x)) = U_m(x).$$

Подставляя $x = m$, получаем

$$f(U_m(m)) = U_m(m),$$

то есть $n = U_m(m)$.
И всё бы было хорошо, если бы $U_m(m)$ было всегда определено. Но вернёмся в суровую реальность и докажем истинное утверждение теоремы Клини.
Вместо равенства чисел нужно рассматривать эквивалентность следующего вида: $n \sim m$, если $U_n = U_m$.
Рассмотрим вычислимую функцию

$$V(m, x) = U_{f(U_m(m))}(x).$$

По свойству главности нумерации U найдётся тотальная вычислимая функция s такая, что

$$V(m, x) = U_{s(m)}(x).$$

Значит, можем записать, что

$$f(U_m(m)) \sim s(m).$$

Важно отметить, что $s(m)$ тотальна. Какое бы значение m мы не подставили, наше утверждение сохранит истинность в силу того, что правая часть уравнения определена.
Теперь, зная, что $s(m)$ вычислима, запишем её как $U_k(m)$

$$f(U_m(m)) \sim U_k(m),$$

и подставим $m = k$

$$f(U_k(k)) \sim U_k(k).$$

Чудесным образом получили слева и справа вполне определённые значения, так как и f, и U_k являются тотальными функциями. То есть, неподвижной точкой (в смысле определённой нами эквивалентности, а не обычного равенства) функции f является $U_k(k)$, совершенно точно определённое значение. □

9 Теорема Райса-Успенского.

10 Определение машин Тьюринга и вычислимых на машинах Тьюринга функций. Тезис Черча-Тьюринга. Неразрешимость проблемы остановки машины Тьюринга.

11 Неразрешимость проблемы достижимости в односторонних в ассоциативных исчислениях. Полугруппы, заданные порождающими и соотношениями. Теорема Маркова-Поста: неразрешимость проблемы равенства слов в некоторой конечно определенной полугруппе (без доказательства).

12 Исчисление высказываний (аксиомы и правила вывода), понятие вывода. Теорема корректности исчисления высказываний.

13 Вывод из гипотез. Лемма о дедукции. Полезные производные правила.

14 Теорема полноты исчисления высказываний.

15 Исчисление резолюций для опровержения пропозициональных формул в КНФ: дизъюнкты, правило резолюций, опровержение КНФ в исчислении резолюций. Теорема корректности исчисления резолюций (для пропозициональных формул в КНФ).

16 Теорема полноты исчисления резолюций (для пропозициональных формул в КНФ). Доказательство нужно знать только для конечных и счетных множеств формул.

17 Полиномиальный алгоритм сведения задачи распознавания совместности конечных множеств произвольных формул к задаче распознавания совместности конечных множеств дизъюнктов.

18 Определение формулы первого порядка в данной сигнатуре. Свободные и связанные вхождения переменных. Интерпретации данной сигнатуры. Общезначимые и выполнимые формулы. Равносильные формулы.

19 Теории и их модели. Семантическое следования. Теорема Черча об алгоритмической неразрешимости отношения семантического следования и общезначимости формул (в доказательстве теоремы можно использовать существование конечно определенной полугруппы с неразрешимой проблемой равенства).

20 Дизъюнкты, универсальные дизъюнкты. Исчисление резолюций (ИР) для доказательства несовместности множеств универсальных дизъюнктов. Теорема корректности ИР.

21 Непротиворечивые теории. Теорема полноты ИР (для множеств универсальных дизъюнктов).

22 Исчисление резолюций для теорий, состоящих из формул общего вида (приведение к предваренной нормальной форме и сколемизация). Доказательства общезначимости с помощью ИР. Выводимость формулы в теории с помощью ИР. Теорема компактности.

23 Гомоморфизмы, эпиморфизмы (сюръективные гомоморфизмы), изоморфизмы. Теорема о сохранении истинности при эпиморфизме. Изоморфные модели. Элементарно эквивалентные модели, элементарная эквивалентность изоморфных моделей.

24 Выразимые (определимые) в данной модели отношения. Теорема о сохранении автоморфизмами выразимых предикатов. Доказательства невыразимости с помощью автоморфизмов.

25 Нормальные модели. Аксиомы равенства. Теорема о существовании нормальных моделей у непротиворечивых теорий, содержащих аксиомы равенства.

26 Игра Эренфойхта для данной пары моделей данной сигнатуры. Теорема об элементарной эквивалентности моделей, для которых в игре Эренфойхта Консерватор имеет выигрышную стратегию.

27 Семантически полные теории. Критерий семантической полноты теории в терминах элементарной эквивалентности моделей. Аксиоматизация элементарной теории упорядоченного множества рациональных чисел.

28 Семантически полные теории. Критерий семантической полноты теории в терминах элементарной эквивалентности моделей. Аксиоматизация элементарной теории упорядоченного множества целых чисел.