

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 непечислимых множеств.	4
1.1	Определение вычислимой частичной функции из \mathbb{N} в \mathbb{N}	4
1.2	Счетность семейств частичных вычислимых функций, и существование невычислимых функций.	4
1.3	Разрешимость подмножества \mathbb{N}	4
1.4	Перечислимые подмножества \mathbb{N}	4
1.5	Счетность семейства перечислимых множеств, и существование непечислимых множеств.	5
2	Эквивалентные определения перечислимости (полуразрешимость, область определения вычислимой функции, множество значений вычислимой функции).	6
3	Теорема Поста. Теорема о графике.	7
3.1	Теорема Поста	7
3.2	Теорема о графике	7
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.	8
4.1	Универсальные вычислимые функции (нумерации) для семейства частичных вычислимых функций натурального элемента.	8
4.2	Несуществование универсальной вычислимой функции для семейства тотальных вычислимых функций натурального аргумента (диагональное рассуждение).	8
4.3	Главные универсальные функции.	8
5	Вычислимая функция, не имеющая тотального вычислимого продолжения. Перечислимое неразрешимое множество. Неразрешимость проблемы применимости.	9
5.1	Вычислимая функция, не имеющая тотального вычислимого продолжения.	9
5.2	Перечислимое неразрешимое множество.	9
5.3	Неразрешимость проблемы применимости (остановки).	9
6	Теорема Поста. Существование перечислимого множества, дополнение которого непечисливо. Перечислимые неотделимые множества.	10
6.1	Теорема Поста	10
6.2	Существование перечислимого множества, дополнение которого непечисливо.	10
6.3	Перечислимые неотделимые множества.	10
7	Сводимости: m-сводимость и Тьюрингова сводимость. Их свойства. Полные перечислимые множества.	11
7.1	m -сводимость и ее свойства.	11
7.2	Тьюрингова сводимость и ее свойства.	11
7.3	Полные перечислимые множества.	11
8	Теорема Клини о неподвижной точке.	12

9	Теорема Райса-Успенского.	13
10	Определение машин Тьюринга и вычислимых на машинах Тьюринга функций. Тезис Черча-Тьюринга. Неразрешимость проблемы остановки машины Тьюринга.	14
10.1	Определение машин Тьюринга и вычислимых на машинах Тьюринга функций.	14
10.2	Тезис Черча-Тьюринга.	14
10.3	Неразрешимость проблемы остановки машин Тьюринга.	14
11	Неразрешимость проблемы достижимости в односторонних ассоциативных исчислениях. Полугруппы, заданные порождающими и соотношениями. Теорема Маркова-Поста: неразрешимость проблемы равенства слов в некоторой конечно определенной полугруппе (без доказательства).	15
11.1	Неразрешимость проблемы достижимости в односторонних ассоциативных исчислениях. . .	15
11.2	Полугруппы, заданные порождающими и соотношениями.	15
11.3	Теорема Маркова-Поста: неразрешимость проблемы равенства слов в некоторой конечно определенной полугруппе (без доказательства).	15
12	Исчисление высказываний (аксиомы и правила вывода), понятие вывода. Теорема корректности исчисления высказываний.	16
12.1	Исчисление высказываний (аксиомы и правила вывода), понятие вывода.	16
12.2	Теорема корректности исчисления высказываний.	16
13	Вывод из гипотез. Лемма о дедукции. Полезные производные правила.	17
13.1	Вывод из гипотез.	17
13.2	Лемма о дедукции.	17
13.3	Полезные производные правила.	18
14	Теорема полноты исчисления высказываний.	19
14.1	Теорема полноты исчисления высказываний.	19
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).	20
16	Теорема полноты исчисления резолюций (для пропозициональных формул в КНФ). Доказательство нужно знать только для конечных и счетных множеств формул.	21
17	Полиномиальный алгоритм сведения задачи распознавания совместности конечных множеств произвольных формул к задаче распознавания совместности конечных множеств дизъюнктов.	22
18	Определение формулы первого порядка в данной сигнатуре. Свободные и связанные вхождения переменных. Интерпретации данной сигнатуры. Общезначимые и выполнимые формулы. Равносильные формулы.	23
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).	24
20	Дизъюнкты, универсальные дизъюнкты. Исчисление резолюций (ИР) для доказательства несовместности множеств универсальных дизъюнктов. Теорема корректности ИР.	25
21	Непротиворечивые теории. Теорема полноты ИР (для множеств универсальных дизъюнктов).	26

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.	27
23	Гомоморфизмы, эпиморфизмы (сюръективные гомоморфизмы), изоморфизмы. Теорема о сохранении истинности при эпиморфизме. Изоморфные модели. Элементарно эквивалентные модели, элементарная эквивалентность изоморфных моделей.	28
24	Выразимые (определимые) в данной модели отношения. Теорема о сохранении автоморфизмами выразимых предикатов. Доказательства невыразимости с помощью автоморфизмов.	29
25	Нормальные модели. Аксиомы равенства. Теорема о существовании нормальных моделей у непротиворечивых теорий, содержащих аксиомы равенства.	30
26	Игра Эренфойхта для данной пары моделей данной сигнатуры. Теорема об элементарной эквивалентности моделей, для которых в игре Эренфойхта Консерватор имеет выигрышную стратегию.	31
27	Семантически полные теории. Критерий семантической полноты теории в терминах элементарной эквивалентности моделей. Аксиоматизация элементарной теории упорядоченного множества рациональных чисел.	32
28	Семантически полные теории. Критерий семантической полноты теории в терминах элементарной эквивалентности моделей. Аксиоматизация элементарной теории упорядоченного множества целых чисел.	33

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 непечислимых 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 $x \in \text{dom } f$ выписывает $f(x)$ и завершается, а на любом входе $x \in A \setminus \text{dom } f$ 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. \square

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. \square

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 перечисливо, если есть программа, на пустом входе последовательно выписывающая все элементы A и только их.

1.5 Счетность семейства перечислимых множеств, и существование непечислимых 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 непечислимые множества $A \subseteq \mathbb{N}$.*

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

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

Определение 7. Область значений f

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

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. $\text{dom } f = A$.
4. $\exists f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, f вычислимая, т.ч. $\text{rng } f = A$.

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 $\text{dom } w_A = A$.

3) \Rightarrow 4)

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

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

Функция g вычислима (т.к. f вычислима), более того $\text{rng } g = \text{dom } f$.

4) \Rightarrow 1)

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

3 Теорема Поста. Теорема о графике.

3.1 Теорема Поста

Теорема 1 (Теорема Поста). *Множества A и \bar{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 $w_{\bar{A}}(x)$, т.к. $x \in A \vee x \in \bar{A}$, то какой-то один из алгоритмов вернет 1 на каком-то шаге. Если это будет w_A , то вернем 1, если же $w_{\bar{A}}$, то вернем 0.

\Leftarrow

Очевидно, из разрешимости следует перечислимость. Если A разрешимо, то и \bar{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 $\Gamma_f = \{(x, f(x)) \mid x \in \text{dom } f\}$.

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 $\text{dom } f$ вычислима и, следовательно, есть вычислимая функция g , т.ч. $\text{rng } g = \text{dom } f$. Рассмотрим функцию $h : \mathbb{N} \rightarrow \mathbb{N}^2$, т.ч. $h(x) \simeq (g(x), f(g(x)))$ для всех $x \in \mathbb{N}$. Она вычислима, причем

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

для всех $x, y \in \mathbb{N}$. Значит, $\Gamma_f = \text{rng } h$, 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 $x \in \text{dom } f$. \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. Функцией $U : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ 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 $s : \mathbb{N} \rightarrow \mathbb{N}$, 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.

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 $n \in \text{dom } d$. 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. \square

5.2 Перечислимое неразрешимое множество.

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

Доказательство. Перечислимость очевидна, поскольку $K = \text{dom } d$, 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

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

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

5.3 Неразрешимость проблемы применимости (остановки).

Определение 11. *Задача разрешения множества $S := \{(n, x) \mid U(n, x) \text{ определено}\}$ 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 $\{x \mid U_x(x) \text{ определено}\}$, для которого доказана неразрешимость. \square

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

6.1 Теорема Поста

Теорема 4 (Теорема Поста). *Множества A и \bar{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 $w_{\bar{A}}(x)$, т.к. $x \in A \vee x \in \bar{A}$, то какой-то один из алгоритмов вернет 1 на каком-то шаге. Если это будет w_A , то вернем 1, если же $w_{\bar{A}}$, то вернем 0.

\Leftarrow

Очевидно, из разрешимости следует перечислимость. Если A разрешимо, то и \bar{A} разрешимо. \square

6.2 Существование перечислимого множества, дополнение которого неперечислимо.

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

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

6.3 Перечислимые неотделимые множества.

Определение 12. *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 разрешимым множеством.*

Доказательство. Рассмотрим множества $A = \{x \mid U_x(x) = 0\}$, $B = \{x \mid U_x(x) = 1\}$. Они перечислимы и не пересекаются. Пусть они отделяются разрешимым множеством C , причем $A \subseteq C$. Тогда функция

$$\chi_C(x) = \begin{cases} 1, & \text{если } U_x(x) = 0 \\ 0, & \text{если } U_x(x) = 1 \\ \alpha(x) \in \{0, 1\}, & \text{иначе} \end{cases}$$

вычислима. Следовательно, $\exists n \in \mathbb{N}$, т.ч. $\chi_C = U_n$. Тогда получаем, что $U_n(n) = 1$, если $U_n(n) = 0$ и $U_n(n) = 0$, если $U_n(n) = 1$. Противоречие. \square

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

7.1 m -сводимость и ее свойства.

Определение 13. Пусть $A, B \subseteq \mathbb{N}$. Множество A m -сводится к множеству B , если существует тотальная вычислимая функция f такая, что $\forall x \in \mathbb{N} (x \in A \Leftrightarrow f(x) \in B)$. Обозначение: $A \leq_m B$.

m -сводимость позволяет построить алгоритм разрешения множества A , если есть алгоритм разрешения множества B : $\chi_A(x) = \chi_B(f(x))$.

Утверждение 11. Свойства:

1. $A \leq_m A$
2. $A \leq_m B \wedge B \leq_m C \Rightarrow A \leq_m C$
3. $\begin{cases} A \leq_m B \\ B \text{ разрешимо} \end{cases} \Rightarrow A \text{ разрешимо}$
4. $\begin{cases} A \leq_m B \\ A \text{ неразрешимо} \end{cases} \Rightarrow B \text{ неразрешимо}$

7.2 Тьюрингова сводимость и ее свойства.

Определение 14. Пусть $A, B \subseteq \mathbb{N}$. Множество A T -сводится к множеству B , если при помощи алгоритма вычисления χ_B можно вычислить χ_A . Обозначение: $A \leq_T B$.

Если $A \leq_m B$, то $A \leq_T B$. Но, обратное утверждение неверно.

Тьюрингова сводимость обладает такими же свойствами, что и m -сводимость.

Помимо этого: $A \leq_T \mathbb{N} \setminus A$, что неверно для m -сводимости.

7.3 Полные перечислимые множества.

Определение 15. Перечислимое множество, к которому m -сводится любое другое перечислимое множество, называется полным перечислимым множеством.

Утверждение 12. Существует полное перечислимое множество

Доказательство. Рассмотрим множество $S = \{(n, x) \mid U_n(x) \text{ определено}\}$. Понятно, что оно перечислимо. Пусть множество $A \in \mathbb{N}$ перечислимо. Покажем, что A m -сводится к S .

Так как A перечислимо, то $\exists f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, т.ч. f вычислима и $\text{dom } f = A$. Тогда $\exists n \in \mathbb{N} U_n = f$. Положим $g(x) = (n, x)$, тогда $\forall x \in \mathbb{N} (x \in A \Leftrightarrow g(x) \in S)$. \square

8 Теорема Клини о неподвижной точке.

Теорема 5 (Теорема Клини о неподвижной точке). Пусть U – главная универсальная вычислимая функция, и вычислимая функция $f : \mathbb{N} \rightarrow \mathbb{N}$ тотальна. Тогда существует $n \in \mathbb{N}$, т.ч. $U_n = U_{f(n)}$, т.е. $\forall x U(n, x) \simeq U(f(n), x)$.

Доказательство. Рассмотрим функцию $V : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$, т.ч.

$$V(k, x) \simeq U(U(k, k), x)$$

для всех $k, x \in \mathbb{N}$. Она, очевидно, вычислима. Вследствие главности U , найдется тотальная вычислимая функция $s : \mathbb{N} \rightarrow \mathbb{N}$, для которой при любых $k, x \in \mathbb{N}$ верно

$$U(s(k), x) \simeq V(k, x) \simeq U(U(k, k), x)$$

Тогда функция $f \circ s$ также тотальная вычислимая. Следовательно, существует $t \in \mathbb{N}$, т.ч. $f \circ s = U_t$. Для любых $x \in \mathbb{N}$ имеем

$$U(s(t), x) \simeq U(U(t, t), x) \simeq U(f(s(t)), x)$$

Положив $n = s(t)$, имеем

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

□

9 Теорема Райса-Успенского.

Теорема 6 (Теорема Райса-Успенского). Пусть нумерация U главная и множество \mathcal{F} вычислимых функций одного аргумента нетривиально (т.е. найдется $f \in F$ и найдется вычислимая $g \notin F$). Тогда множество индексов

$$F = \{n \mid U_n \in \mathcal{F}\}$$

неразрешимо.

Доказательство. Пусть $g \in \mathcal{F}$ и $h \notin \mathcal{F}$ и множество F разрешимо. Пусть $g = U_k$ и $h = U_m$. Определим функцию f

$$f(n) = \begin{cases} m, & \text{если } n \in F \\ k, & \text{если } n \notin F \end{cases}$$

для всех $n \in \mathbb{N}$. Так как F разрешимо, то тотальная функция f вычислима. Тогда, по теореме Клини о неподвижной точке, найдется число $n \in \mathbb{N}$, т.ч. $U_{f(n)} = U_n$. Если $n \in F$, то $U_n \in \mathcal{F}$, но $U_n = U_{f(n)} = U_m = h \notin \mathcal{F}$. Если же $n \notin F$, то $U_n \notin \mathcal{F}$, следовательно, $U_n = U_{f(n)} = U_k = g \in \mathcal{F}$. Противоречие. Значит, F неразрешимо. \square

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

10.1 Определение машин Тьюринга и вычислимых на машинах Тьюринга функций.

Определение 16. *Машина Тьюринга задается*

- *непустым конечным алфавитом Σ , среди которого выделен пробельный символ и не содержащее пробельного символа множества Γ – входной алфавит;*
- *непустым конечным множеством состояний Q , среди которого выделено начальное состояние s_0 и множество терминальных состояний $F \subseteq Q$;*
- *функций переходов $\delta : (Q \setminus F) \times \Sigma \rightarrow Q \times \Sigma \times \{-1, 0, 1\}$.*

Машина Тьюринга состоит из бесконечной ленты, разбитой на ячейки, головки, в любой момент времени указывающей на одну ячейку и одной ячейки памяти, в которой хранится текущее состояние. В начальный момент времени на ленте записано некоторое слово, составленной из букв входного алфавита, головка смотрит на первый символ этого слова, во всех остальных ячейках пробелы. Затем в каждый момент времени вычисляется $\delta(q, c) = (q', c', \Delta)$, где q – текущее состояние, c – символ записанный в ячейке, на которую сейчас смотрит головка. Состояние меняется на q' , символ в текущей ячейке на c' , головка остается на месте или передвигается на один влево или вправо в соответствии со значением Δ . Если $q' \in F$, то работа машины заканчивается, иначе этот процесс продолжается.

Машины Тьюринга естественным образом отождествляются с частичными функциями $f : \Gamma^* \rightarrow \Gamma^*$ – аргументом функции является входное слово, а возвращает функция слово, записанное на ленте после завершения работы машины. Функции, которые можно таким образом получить по некоторой машине Тьюринга, называются *вычислимыми на машине Тьюринга*.

10.2 Тезис Черча-Тьюринга.

Утверждение 13 (Тезис Черча-Тьюринга). *Любая вычислимая функция вычислима на машине Тьюринга.*

Здесь понятие «вычислимая функция» используется в неформальном смысле, под ним понимается функция, вычислимая в любой разумной модели, которая может прийти нам в голову. Тезис не является формальным утверждением, он никак не доказывается и принимается нами на веру.

10.3 Неразрешимость проблемы остановки машин Тьюринга.

Утверждение 14. *Не существует вычислимой функции, определяющей по машине Тьюринга и входному слову, остановится ли эта машина.*

Доказательство. Следует из утверждения о существовании полного перечислимого множества. □

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

Теорема 7 (Теорема Маркова-Поста).

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

12.1 Исчисление высказываний (аксиомы и правила вывода), понятие вывода.

Определение 17. Высказыванием называется утверждение, которое либо истинно, либо ложно. При этом если A, B являются высказываниями, то $\neg A, A \vee B, A \wedge B, A \rightarrow B$ – тоже высказывания.

Определение 18. Выводом называется конечная последовательность формул, каждая из которой либо является аксиомой, либо получается из ранее встретившихся по правилам вывода.

Имеется 11 аксиом:

1. $A \rightarrow (B \rightarrow A)$: истинна следует из чего угодно.
2. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$: левая дистрибутивность импликации относительно самой себя
3. $(A \wedge B) \rightarrow A$;
4. $(A \wedge B) \rightarrow B$: из конъюнкции двух формул следует каждая из формул.
5. $A \rightarrow (B \rightarrow (A \wedge B))$: если выполнены обе формулы, то выполнена их конъюнкция.
6. $A \rightarrow (A \vee B)$;
7. $B \rightarrow (A \vee B)$: дизъюнкция двух формул следует из каждой из них.
8. $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C))$: если формула C следует из каждой из формул A и B , то она следует и из их дизъюнкции.
9. $\neg A \rightarrow (A \rightarrow B)$: из лжи следует все, что угодно.
10. $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$: правило рассуждения от противного, если из A следует B и $\neg B$, то само A обязано быть неверным.
11. $A \vee \neg A$: закон исключенного третьего.

В качестве единственного правила вывода выступает *modus ponens*:

$$\frac{A \quad A \rightarrow B}{B}$$

Понимается оно так: если ранее уже выведены формулы A и $A \rightarrow B$, то в вывод можно приписать B .

Буквами A, B, C могут быть обозначены любые формулы.

Утверждение о том, что формула φ выводима в исчислении высказываний (ИВ), записывается так: $\vdash \varphi$.

12.2 Теорема корректности исчисления высказываний.

Определение 19. Формула называется тавтологией, если она как булева формула верна при всех значениях входящих в нее переменных.

Теорема 8 (Теорема корректности исчисления высказываний). Если $\vdash \varphi$, то φ – тавтология.

Доказательство. Любая аксиома является тавтологией. Это можно проверить непосредственно по таблице истинности. Если A и $A \rightarrow B$ являются тавтологиями, то B также является тавтологией: только при $A = B = 1$ верны и формула A и импликация $A \rightarrow B$. Индукцией по номеру формулы в выводе доказывается, что все формулы в выводе тавтологичны, что и требовалось. \square

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

13.1 Вывод из гипотез.

Определение 20. Пусть Γ – некоторое множество формул. Тогда выводом из множества посылок Γ называется последовательность формул, каждая из которых является либо аксиомой, либо элементом Γ , либо выводится из более ранних формул по правилу *modus ponens*. Если формула A встречается в некотором выводе из Γ , то она называется выводимой из Γ . Обозначение: $\Gamma \vdash A$.

13.2 Лемма о дедукции.

Лемма 1. $\vdash A \rightarrow A$.

Доказательство. Вывод состоит из 5 формул:

1. $A \rightarrow ((A \rightarrow A) \rightarrow A)$ (аксиома 1)
2. $A \rightarrow (A \rightarrow A)$ (аксиома 1)
3. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ (аксиома 2)
4. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ (modus ponens 1, 3)
5. $A \rightarrow A$ (modus ponens 2, 4)

□

Теорема 9 (Лемма о дедукции). Из множества посылок выводится импликация $A \rightarrow B$ тогда и только тогда, когда при добавлении A к списку посылок выводится B . Иначе говоря, $\Gamma \vdash A \rightarrow B \Leftrightarrow \Gamma \cup \{A\} \vdash B$.

Доказательство. \Rightarrow

Действительно, если к выводу импликации $A \rightarrow B$ из Γ добавить формулы A и B , то получится вывод B из $\Gamma \cup \{A\}$: формулу A можно написать как посылку, а B – по modus ponens.

\Leftarrow

Будем доказывать по индукции такое утверждение: если C_1, \dots, C_n есть вывод из $\Gamma \cup \{A\}$, то для всех i импликация $A \rightarrow C_i$ выводима из Γ . Рассуждение по индукции будет опираться на такой принцип, объединяющий в себе и базу, и переход: если импликация $A \rightarrow C_1, \dots, A \rightarrow C_{i-1}$ выводимы, то и $A \rightarrow C_i$ тоже выводима. Разберем несколько случаев:

- C_i является аксиомой. В таком случае импликация выводится в три шага: C_i ; $C_i \rightarrow (A \rightarrow C_i)$ (аксиома 1); $A \rightarrow C_i$ (modus ponens предыдущих двух)
- C_i является посылкой, т.е. элементом $\Gamma \cup \{A\}$.
 - $C_i \in \Gamma$. Годится тот же вывод, что и для аксиомы.
 - $C_i = A$. Импликация $A \rightarrow A$ выводится по лемме.
- C_i выводится по правилу modus ponens из формул C_j и C_k для некоторых $j, k < i$. В этом случае C_k обязательно имеет вид $C_k \rightarrow C_i$, иначе modus ponens не применить. По предположению индукции $\Gamma \vdash C_j$ и $\Gamma \vdash C_k$, т.е. $\Gamma \vdash A \rightarrow (C_j \rightarrow C_i)$. Далее добавим в вывод вторую аксиому: $(A \rightarrow (C_j \rightarrow C_i)) \rightarrow ((A \rightarrow C_j) \rightarrow (A \rightarrow C_i))$ – и двумя применениями modus ponens получим $A \rightarrow C_i$, что и требовалось.

Все случаи разобраны, поэтому индукционный принцип установлен и теорема доказана.

□

13.3 Полезные производные правила.

Утверждение 15. *Справедливы следующие правила вывода (каждый раз сверху от горизонтальной черты записаны условия теоремы, а снизу – утверждение) – следствия леммы о дедукции:*

1. Правило вывода конъюнкции: $\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$;
2. Правило рассуждения от противного: $\frac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$;
3. Правило разбора случаев: $\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$.

14 Теорема полноты исчисления высказываний.

14.1 Теорема полноты исчисления высказываний.

Лемма 2 (Базовая). *Имеют место следующие выводимости:*

$$\begin{array}{llll}
 A, B \vdash A \wedge B & A, B \vdash A \vee B & A, B \vdash A \rightarrow B & \\
 A, \neg B \vdash \neg(A \wedge B) & A, \neg B \vdash A \vee B & A, \neg B \vdash \neg(A \rightarrow B) & A \vdash \neg(\neg A) \\
 \neg A, B \vdash \neg(A \wedge B) & \neg A, B \vdash A \vee B & \neg A, B \vdash A \rightarrow B & \neg A \vdash \neg A \\
 \neg A, \neg B \vdash \neg(A \wedge B) & \neg A, \neg B \vdash \neg(A \vee B) & \neg A, \neg B \vdash A \rightarrow B &
 \end{array}$$

Доказательство. Слева от знака выводимости стоят либо формулы, либо отрицания формул A и B . Справа стоит более сложная формула или ее отрицание в зависимости от того, что из двух верно, если верны обе посылки.

Все 14 утверждений очень простые и выводятся из аксиом за несколько шагов. \square

Следующая лемма обобщает предыдущую.

Лемма 3 (Основная). *Пусть A – формула, $x \in \{0, 1\}$. Через A^x обозначим формулу A , если $x = 1$, и формулу $\neg A$, если $x = 0$. Далее, пусть Φ – формула от n переменных, выражающая функцию φ . Тогда для всех x_1, \dots, x_n выполнено*

$$A_1^{x_1}, \dots, A_n^{x_n} \vdash \Phi(A_1, \dots, A_n)^{\varphi(x_1, \dots, x_n)}$$

Доказательство. Будем доказывать индукцией по построению формулы. В качестве базы возьмем $\Phi(A_1, \dots, A_n) = A_i$. Тогда $\varphi(x_1, \dots, x_n) = x_i$ и в правой части стоит просто одна из посылок.

Теперь докажем переход. Для разных связок он делается одинаково, возьмем для примера конъюнкцию. Таким образом, формула Φ есть конъюнкция $\Psi \wedge \Omega$, а φ есть также конъюнкция функций ψ и ω , но уже в смысле булевой функции, а не синтаксической связки. По предположению индукции имеем $A_1^{x_1}, \dots, A_n^{x_n} \vdash \Psi(A_1, \dots, A_n)^{\psi(x_1, \dots, x_n)}$ и $A_1^{x_1}, \dots, A_n^{x_n} \vdash \Omega(A_1, \dots, A_n)^{\omega(x_1, \dots, x_n)}$. Далее по базовой лемме имеем

$$\Psi(A_1, \dots, A_n)^{\psi(x_1, \dots, x_n)}, \Omega(A_1, \dots, A_n)^{\omega(x_1, \dots, x_n)} \vdash (\Psi \wedge \Omega)(A_1, \dots, A_n)^{(\psi \wedge \omega)(x_1, \dots, x_n)}.$$

Последняя формула есть $\Phi(A_1, \dots, A_n)^{\varphi(x_1, \dots, x_n)}$. Далее получаем, что $A_1^{x_1}, \dots, A_n^{x_n} \vdash \Phi(A_1, \dots, A_n)^{\varphi(x_1, \dots, x_n)}$, что и требовалось. Переходы для остальных связок доказываются аналогично. Таким образом, индуктивное утверждение доказано. \square

Теорема 10 (Теорема полноты исчисления высказываний). *Пусть формула Φ , зависящая от переменных p_1, \dots, p_n , является тавтологией. Тогда $\vdash \Phi$.*

Доказательство. Поскольку формула Φ является тавтологией, она выражает функцию φ , тождественно равную единице. По основной лемме для любого набора $(x_1, \dots, x_n) \in \{0, 1\}^n$ выполнено $p_1^{x_1}, \dots, p_n^{x_n} \vdash \Phi$. При помощи обратной индукции докажем, что для каждого k от 0 до n выполнено $p_1^{x_1}, \dots, p_k^{x_k} \vdash \Phi$. Начальное утверждение (для $k = n$) у нас уже есть. Конечное (для $k = 0$) утверждает $\vdash \Phi$, что и требуется. Осталось доказать переход.

Пусть для некоторого k утверждение уже доказано. Докажем для $k-1$. Из полученного имеем $p_1^{x_1}, \dots, p_k^{x_k} \vdash \Phi$ и $p_1^{x_1}, \dots, \neg p_k \vdash \Phi$. По правилу исчерпывающего разбора случаев получаем $p_1^{x_1}, \dots, p_{k-1}^{x_{k-1}} \vdash \Phi$, что и требовалось. Таким образом, теорема о полноте доказана. \square

- 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.