Дискретная математика. Коллоквиум весна 2017. Теоремы

...

12 марта 2017 г.

Содержание

Теорема 1

Теорема. *Пусть* $(\Omega,\mathfrak{F},\mathcal{P})(\Omega,\mathfrak{F},\mathcal{P})$ *— вероятностное пространство. Тогда для произвольных событий* $A_1,A_2,\ldots,A_nA_1,A_2,\ldots,A_n$ *справедлива формула*

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_i \mathcal{P}(A_i) - \sum_{i<j} \mathcal{P}(A_i \cap A_j) + \sum_{i<j<k} \mathcal{P}(A_i \cap A_j \cap A_k) + \ldots + (-1)^{n-1}\,\mathcal{P}\left(\bigcap_{i=1}^{n} A_i\right).\mathcal{P}\left(\bigcup_{i=1}^{n}\right.$$

$\sum_i \mathcal{P}(A_i) - \sum_{i<j} \mathcal{P}(A_i \cap A_j) + \sum_{i<j<k} \mathcal{P}(A_i \cap A_j \cap A_k) + \ldots + (-1)^{n-1}\,\mathcal{P}\left(\bigcap_{i=1}^{n} A_i\right)$.

Доказательство. Её можно получить из принципа включений-исключений в форме индикаторных функций:

$$\mathbf{1}_{\bigcup_i A_i} = \sum_i \mathbf{1}_{A_i} - \sum_{i<j} \mathbf{1}_{A_i \cap A_j} + \sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} + \ldots + (-1)^{n-1}\,\mathbf{1}_{A_1 \cap \ldots \cap A_n}.\mathbf{1}_{\bigcup_i A_i} = \sum_i \mathbf{1}_{A_i} - \sum_{i<j} \mathbf{1}_{A_i \cap A_j} +$$

$\sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} + \ldots + (-1)^{n-1}\,\mathbf{1}_{A_1 \cap \ldots \cap A_n}$.

Пусть A_iA_i — события вероятностного пространства $(\Omega,\mathfrak{F},\mathcal{P})(\Omega,\mathfrak{F},\mathcal{P})$, то есть $A_i \in \mathfrak{F}A_i \in \mathfrak{F}$. Возьмем математическое ожидание $\mathcal{M}\mathcal{M}$ от обеих частей этого соотношения, и, воспользовавших линейностью математического ожидания и равенством $\mathcal{P}(A) = \mathcal{M}(\mathbf{1}_A)\mathcal{P}(A) = \mathcal{M}(\mathbf{1}_A)$ для произвольного события $A \in \mathfrak{F}A \in \mathfrak{F}$, получим формулу включения-исключения для вероятностей.

[:|||:]

Теорема 2

Теорема. *Условную вероятность* $Pr[A|B]$ *можно вычислить по формуле Байеса:*

$$Pr[A|B] = \frac{Pr[B|A]}{Pr[B]} \cdot Pr[A]$$

Доказательство.

$$Pr[A|B] = \frac{Pr[B|A]}{Pr[B]} \cdot Pr[A]$$

$$\Updownarrow$$

$$Pr[A|B] \cdot Pr[B] = Pr[B|A] \cdot Pr[A]$$

$$\Updownarrow$$

$$\frac{Pr[A \cap B]}{Pr[B]} \cdot Pr[B] = \frac{Pr[B \cap A]}{Pr[A]} \cdot Pr[A]$$

$$\Updownarrow$$

$$Pr[A \cap B] = Pr[B \cap A]$$

Т.к. $A \cap B = B \cap A$, то последнее равенство верно, а значит верна формула Байеса. **[:|||:]**

Теорема 3

Теорема. *Условной вероятностью события A при условии события B называется* $\mathbb{P}(A \mid B) = \dfrac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$*, где* $\mathbb{P}(A \cap B)\mathbb{P}(A \cap B)$ *— вероятность наступления обоих событий сразу.*

Доказательство. Пусть ровно r исходов события B входят и в событие A. Исходы события B уже реализовались В данном испытании произошло одно из t событий, входящих в B. Все элементарные события равновероятны, следовательно, для данного испытания вероятность наступления произвольного элементарного события, входящего в B равна 1/t. Тогда по классическому определению вероятности, в данном испытании событие A произойдет с вероятностью r/t. $P(A|B) = \frac{\frac{r}{m}}{\frac{t}{m}} = \frac{P(AB)}{PB}$

[:|||:]

Теорема 4

Теорема. *Математическое ожидание E линейно.*

Доказательство. Пусть ξ и η — случайные величины, заданные на одном вероятностном пространстве. Тогда выполняется равенство

$$E(\xi + \eta) = \sum_w (\xi(w) + \eta(w))p(w) = \sum_w \xi(w)p(w) + \sum_w \eta(w)p(w) = E(\xi) + E(\eta)$$

То есть математическое ожидание суммы случайных величин равно сумме математического ожидания каждой из этих величин. Пусть теперь ξ — случайная величина, α — действительное число. Тогда выполняется равенство

$$E(\alpha \cdot \xi) = \sum_w (\alpha \cdot \xi(w)p(w)) = \alpha \cdot \sum_w \xi(w)p(w) = \alpha \cdot E(\xi)$$

То есть математическое ожидание произведения константы и случайной величины равно произведению этой константы и математического ожидания самой величины.
Таким образом, линейность математического ожидания доказана. **[:|||:]**

Теорема 5

Неравенство Маркова в теории вероятностей дает оценку вероятности, что случайная величина превзойдет по модулю фиксированную положительную константу, в терминах её математического ожидания. Получаемая оценка обычно груба, однако она позволяет получить определённое представление о распределении, когда последнее не известно явным образом.

Теорема. *Пусть случайная величина X:* $\Omega \to \mathbb{R}+$ *определена на вероятностном пространстве* $(\Omega, F, \mathbb{R})$*, и ее математическое ожидание* $\mathbb{E}|\xi| < \infty$*. Тогда* $\forall\ x > 0\ \ \mathbb{P}(|\xi| \geq x) \leq \frac{\mathbb{E}|\xi|}{x}$

Доказательство. Возьмем для доказательства следующее понятие:

Пусть A - некоторое событие. Назовем индикатором события A случайную величину I, равную единице если событие A произошло, и нулю в противном случае. По определению величина I(A) имеет распределение Бернулли с параметром

$p = \mathbb{P}(I(A) = 1) = \mathbb{P}(A)$,

и ее математическое ожидание равно вероятности успеха $p = \mathbb{P}(A)$. Индикаторы прямого и противоположного событий связаны равенством $I(A) + I(\overline{A}) = 1$. Поэтому $|\xi| = |\xi| * I(|\xi| < x) + |\xi| * I(|\xi| \geq x) \geq |\xi| * I(|\xi| \geq x) \geq x * I(|\xi| \geq x)$. Тогда $\mathbb{E}|\xi| \geq \mathbb{E}(x * I(|\xi| \geq x)) = x * \mathbb{P}(|\xi| \geq x)$.

Разделим обе части на x:

$\mathbb{P}(|\xi| \geq x) \leq \frac{\mathbb{E}|\xi|}{x}$

Пример:

Ученики в среднем опаздывают на 3 минуты. Какова вероятность того, что ученик опоздает на 15 минут и более? Дать грубую оценку сверху.

$\mathbb{P}(|\xi| \geq 15) \leq 3/15 = 0.2$

[:|||:]

Теорема 7

Теорема. *Объединение счетного числа счетных или конечных множеств счетно или конечно*

Доказательство. Пусть имеется счётное число счётных множеств A1, A2, . . .

Расположив элементы каждого из них слева направо в последовательность (Ai = ai0, ai1, . . .) и поместив эти последовательности друг под другом, получим таблицу

a00 a01 a02 a03 . . .

a10 a11 a12 a13 . . .

a20 a21 a22 a23 . . .

a30 a31 a32 a33 . . .

. . . . . .

Теперь эту таблицу можно развернуть в последовательность, например, проходя по очереди диагонали: a00, a01, a10, a02, a11, a20, a03, a12, a21, a30, . . . Если множества Ai не пересекались, то мы получили искомое представление для их объединения.

Если пересекались, то из построенной последовательности надо выбросить повторения. Если множеств конечное число или какие-то из множеств конечны, то в этой конструкции части членов не будет — и останется либо конечное, либо счётное множество.

[:|||:]

Теорема 8

Теорема. *Декартово произведение счетных множеств счетно.*

Доказательство. Б.о.о. можно считать, что необходимо доказать счетность $\mathbb{N} \times \mathbb{N}$. Разобьем наше декартово произведение в объединение множеств вида $\{a_0\} \times \mathbb{N}$. Каждое такое множество счетно. В итоге декартово произведение разложилось в счетное объединение счетных множеств, а значит и само счетно. **[:|||:]**

Теорема 10

Если для множества A и B существует инъекция из A в B и инъекция из B в A, то существует и биекция между A и B. Доказательство. Пусть $f : A \to B$ и $g : B \to A$ инъекции. Рассмотрим орграф с вершинами $A \cup B$. Для точек $x \in A$ и $y \in B$ проводим ребро из x в y, если $f(x) = y$ и ребро из y в x, если $g(y) = x$. По построению из каждой точки выходит ровно одно ребро. А так как функции инъективны, то и входит не больше одного.
Разобьем граф на компоненты связности, забыв об ориентации ребер, и рассмотрим каждую компоненту отдельно. Для каждой компоненты есть три варианта: Компонента может быть циклом из стрелок, бесконечной цепочкой стрелок, начинающейся в некоторой вершине или бесконечной в обе стороны цепочкой стрелок.
В нашем графе вершины бывают "левые"(из A) и "правые"(из B). Они чередуются, поэтому цикл может быть только четной длины и содержит поровну вершин из A и из B. Они чередуются, поэтому цикл может быть только четной длины и содержит поровну вершин из A и из B. Любое из отображений f и g может быть использовано чтобы построить биекцию между A и B вершинами цикла. То же самое верно для бесконечной в обе стороны цепочки. Если же цепочка бесконечна только в одну сторону, то для построения биекции годится только одно из отображений. Скажем, если она начинается с a, то нам годится только функция f (при которой a соответствует f(a)). Но в любом случае, одна из функций f и g годится, так что внутри каждой связной компоненты у нас есть биекция, и остается их объединить для всех связных компонент.

Теорема 11

Полнота стандартного базиса. Любое высказывание может быть выражено как дизъюнкция таких высказываний, у котороых ровно в одной строке стоит 1, а в остальных стоят нули. Действительно, выберем все строки таблицы высказывания, в которых стоят единицы. Для каждой такой строки образуем высказывание, которое истинно только в данной строке, а в остальных ложно, дизъюнкция всех этих высказываний и будет выражать искомое.
Теперь научимся выражать через диъюнкции, конъюнкции и отрицания высказывания того вида, который использован в предыдущей конструкции. Чтобы получить высказывание , которое истинно ровно для одного произвольного набора логических значений, сделаем следующее:

Если значение какой-то переменной равно единице, то включим эту переменную в высказывание, а если нулю, то включим ее отрицание. Построенная конъюнкция принимает значение 1 лишь тогда, когда все ее члены равны 1. По построению это происходит ровно на одном наборе значений переменных.

Теорема 12

Существование и единственность полинома Жегалкина. Сначала докажем по индукции, что любое произвольное высказывание $f(x_1 \dots x_n)$ можно выразить формулой со связкам $\wedge, \oplus, 1$. База индукции $n = 1$. Константа 1 уже есть. 0 выражается как $1 \oplus 1$.
Пусть утверждение доказано для всех составных высказываний от n элементарных высказываний. Докажем выразимость для составных высказываний от $n+1$ элементарного высказывания. Для этого по высказыванию $f(x_1, \dots, x_n+1)$ определим два высказывания от n элементарных высказываний, а именно $f_0(x_1, \dots x_n) = f(x_1, \dots, x_n, 0)$ и $f_1(x_1, \dots, x_n) = f(x_1, \dots, x_n, 1)$. По предположению индукции f_0 и f_1 выражаются через базис Жегалкина. Выразим теперь f (разложение Рида): $f = ((1 \oplus x_{n+1}) \wedge f_0) \oplus (x_{n+1} \wedge f_1)$. Действительно, при $x_{n+1} = 0$ обращается в 0 второе слагаемое, при $x_{n+1} = 1$ - первое. В любом случае получаем совпадение левой и правой частей равенства.
Теперь докажем единственность. Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций вида $x_{i_1} \dots x_{i_k}$ существует ровно 2^n, так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных.
Теперь достаточно лишь доказать, что различные полиномы реализуют различные функции. Предположим противное. Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных, и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие. Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом.

Теорема 13

Теорема. *Существует булева фукнция от n переменных схемной сложности* $\Omega(\frac{2^n}{n})$

Доказательство. Докажем, что всякую фукнцию можно вычислить схемой размера не больше $O(n2^n)$.

Для всякого $a \in \{0,1\}^n$ введем фукнцию $f_a(x)$, такую что

$$f_a(x) = \begin{cases} 1, & x = a \\ 0, & \text{иначе} \end{cases}$$

Введем обозначение $x^1 = x, x^0 = \overline{x}$. Тогда такая функция может быть записана следующим образом:

$$f_a(x) = \bigwedge i = 1^n x_i^{a_i}$$

Тогда для произвольной f:

$$f(x) = \bigvee_{a \in f^{-1}(1)} f_a(x)$$

Сначала наша схема должна вычислить отрицание всех элементов, потом вычислить все функции f_a. Для вычисления каждой потребуется $n-1$ раз применить конъюнкцию. Всего в итоге получится $2^n(n-1)$ элемент. В итоге нужно будет взять дизъюнкцию нужных функций. Получим 2^n элементов, и суммарно не более $O(n2^n)$.

[:|||:]

Теорема 15

Схема умножения n-битовых чисел за $O(n^2)$.

Пусть на вход подаются два числа $x = x_{n-1} \dots x_1 x_0$ и $y = y_{n-1} \dots y_1 y_0$. Мы хотим вычислить $z = x \cdot y$. Заметим, что z имеет не больше $2n$ разрядов. Действительно, $x, y < 2^n$, так что $z = x \cdot y < 2^{2n}$, а значит для его записи достаточно $2n$ разрядов.

Для вычисления z воспользуемся школьным методом. В нем умножение двух чисел сводится к сложению n чисел. Действительно, чтобы умножить x на y достаточно для всякого $i = 0, \dots, n-1$ умножить x на y_i, приписать в конце числа i нулей и затем сложить все полученные числа. Умножение x на y_i легко реализуется с помощью n конъюнкций. После этого остается сложить n чисел длины не более $2n$. Для этого мы можем $n-1$ раз применить схему для сложения. Размер каждой схемы для сложений линейный, так что суммарная сложность схемы для умножения получается $O(n^2)$.

Теорема 16

Схема проверки связности графа на n вершинах полиномиального размера.

Пусть матрица A - матрица смежности графа с единицами на главной диагонали. Можно показать, что на пересечении строки i и столбца j матрицы A^k записано число путей длины k из вершины v_i в вершину v_j. Теперь рассмотрим матрицу A', которая отличается от матрицы A тем, что у нее стоят единицы на главной диагонали.

Заметим следующий факт: если между двумя вершинами есть путь длины меньше n - 1, то есть и путь длины ровно $n-1$, достаточно добавить нужное количество петель. То есть надо рассмотреть матрицу $(A')^{n-1}$. Если в яйчеках нет нулей - граф связен, иначе нет. Теперь опишем схему.

На вход схема получает матрицу смежности A'. Схема последовательно вычисляет булевы степени этой матрицы $(A')^2, \ldots, (A')^{n-1}$. Затем схема вычисляет конъюнкцию всех ячеек матрицы $(A')^{n-1}$ и подает ее на выход.

Оценим размер схемы. Для булева умножения достаточно $n^2 \cdot O(n) = O(n^3)$ операций. Всего нам нужо $(n-1)$ умножений, так что для вычисления матрицы $(A')^{n-1}$ достаточно $O(n^4)$ операций. Для последнего этапа - конъюнкции нужно $O(n^2)$ операций. Итого получается $O(n^4) + O(n^2) = O(n^4)$ операций.

Теорема 17

Теорема. *Разрешимые множества перечислимы.*

Доказательство. Алгоритм перечисления множества A использует алгоритм разрешения множества A. Он перебирает все числа, начиная с 0; для каждого числа n вычисляет индикаторную функцию $\chi_A(n)$ и печатает число n, если полученное значение равно 1. Корректность такого алгоритма очевидна из определений. **[:|||:]**

Теорема 18

Теорема. *Множество M и его дополнение $\overline{M}$ разрешимы тогда и только тогда, когда M и $\overline{M}$ перечислимы.*

Доказательство.

Необходимость:
Пусть M и $\overline{M}$ разрешимы. Случаи, когда $M = \mathbb{N}$ или $M = \varnothing$, тривиальны. Будем считать, что $M \neq \varnothing$ и M $\neq \mathbb{N}$. Тогда существуют такие a и b, что $a \in M$ и $b \in \overline{M}$. Поскольку M разрешимо, его характеристическая функция χ_M вычислима. Рассмотрим функцию

$$f(x) = \begin{cases} x \text{ при } \chi_M(x) = 1 \\ a \text{ при } \chi_M(x) = 0 \end{cases}$$

M является множеством значений f: ничего, кроме значений M, в $E(f)$, очевидно, быть не может, а для любого $m \in M$ верно, что $f(m) = m$. Аналогично, рассмотрим функцию

$$g(x) = \begin{cases} x \text{ при } \chi_M(x) = 0 \\ b \text{ при } \chi_M(x) = 1 \end{cases}$$

$\overline{M}$ является областью значений g. Таким образом, M и $\overline{M}$ перечислимы (перечисляющие алгоритмы могут быть, например, устроены так: последовательно для всех натуральных n, начиная с нуля, алгоритм выводит значение $f(n)$ или $g(n)$ соответственно).

Достаточность:
Пусть M и $\overline{M}$ перечислимы. Тогда существуют алгоритмы соответственно $\mathfrak{A}$ и $\mathfrak{B}$, с помощью которых могут быть получены все элементы этих множеств. Рассмотрим алгоритм, запускающий $\mathfrak{A}$ и $\mathfrak{B}$ паралленьно, который выводит сначала первое число, полученное $\mathfrak{A}$, затем — первое число, полученное $\mathfrak{B}$, затем — второе число, полученное $\mathfrak{A}$, и так далее. Такой алгоритм будет являться перечисляющим алгоритмом $\mathbb{N}$, который получает элементы M на нечётных выводах и элементы $\overline{M}$ — на чётных. Соответсвенно, для любого элемента x верно, что он будет выведен рассматриваемым алгоритмом за конечное число шагов. Если он был выведен как нечётный по счёту вывод, то $\chi_M(x) = 1$, если как чётный — $\chi_M(x) = 0$. Таким образом, χ_M вычислима, а значит, M и $\overline{M}$ разрешимы. **[:|||:]**

Теорема 19

Теорема. *Перечислимые множества являются множествами значений вычислимых функций.*

Доказательство. Пусть M — перечислимое множество. Тогда существует алгоритм $\mathfrak{A}$, выводящий все его элементы. Рассмотрим алгоритм, который принимает на вход натуральное число n, после чего запускает $\mathfrak{A}$ и считает его выводы. Дойдя до n-го по счёту (начиная с 0) вывода, алгоритм останавливается, выводя n-й вывод алгоритма $\mathfrak{A}$ как результат своей работы.
Множество значений функции, которую вычисляет вышеописанный алгоритм, будет совпадать с множеством чисел, выводимых $\mathfrak{A}$, то есть с M.

[:|||:]

Теорема 20

Теорема. *Перечислимые множества являются множествами значений всюду определённых вычислимых функций.*

Доказательство. Пусть M — перечислимое множество. Тогда существует алгоритм $\mathfrak{A}$, выводящий все его элементы. Рассмотрим алгоритм, который принимает на вход натуральное число n, после чего запускает $\mathfrak{A}$ и считает его выводы. Дойдя до n-го по счёту (начиная с 0) вывода, алгоритм останавливается, выводя n-й вывод алгоритма $\mathfrak{A}$ как результат своей работы.
Множество значений функции f, которую вычисляет вышеописанный алгоритм, будет совпадать с множеством чисел, выводимых $\mathfrak{A}$, то есть с M. Если множество M бесконечно, то f также будет всюду определённой по построению. Если же M конечно, рассмотрим функцию $f_1(x) = f(x \bmod (l+1))$, где l — номер вывода $\mathfrak{A}$, после которого количество различных выведенных $\mathfrak{A}$ элементов станет равно $[M]$. Значение l будет конечным, так как любой элемент M выводится $\mathfrak{A}$ за конечное число шагов. Данная функция будет всюду определённой, поскольку $\mathfrak{A}$ до своей остановки совершает не менее l шагов, и множество её значений будет совпадать

с M, поскольку по построению в множестве её значений $[M]$ различных элементов, и все они являются результатом работы $\mathfrak{A}$.

[:|||:]

Теорема 21

Теорема. *Множества значений всюду определённых функций перечислимы.*

Доказательство. Пусть $M = f(\mathbb{N})$ — множество значений некоторой всюду определённой функции f. Рассмотрим алгоритм, последовательно выводящий для каждого натурального числа n, начиная с 0, значение $f(n)$. Он будет являться перечисляющий алгоритмом для M: для любого $m \in M$ верно, что $\exists x \in \mathbb{N} : f(x) = m$, следовательно, вышеописанный алгоритм выведет m на своём x-ом шаге. **[:|||:]**

Теорема 22

Теорема. *Множество значений всюду опрелённой вычислимой функции является областью определения вычислимой функции.*

Доказательство. Пусть f — всюду определённая вычислимая функция. Рассмотрим алгоритм, принимающий на вход натуральное число x, который последовательно вычисляет значения $f(n)$ для всех натуральных n, начиная с 0, и, если полученное в какой-то момент значение равно x, выводит 1. Если $x \in E(f)$, то $\exists m \in \mathbb{N} : f(m) = x$. Тогда вышеописанный алгоритм остановится за конечное число шагов: он завершит свою работу, вычислив значения $f(n)$ для всех $n \leqslant m$, а для этого требуется конечное число шагов, поскольку f вычислима и всюду определена. Если же $x \notin E(f)$, то данный алгоритм никогда не остановится, поскольку условие его остановки — существование такого $m \in \mathbb{N}$, что $f(m) = x$. Таким образом, функция, вычисляемая вышеопианным алгоритмом, определена в точности на $E(f)$. **[:|||:]**

Теорема 23

Теорема. *Область определения вычислимой функции является множеством значений вычислимой функции.*

Доказательство. Пусть S – область определения некоторой вычислимой функции f, а p – номер программы, вычисляющей f в нумерации U. Рассмотрим функцию g:

$$g(x,t) = \begin{cases} x & F(p,x,t) = 1 \\ - & F(p,x,t) = 0 \end{cases}$$

Если $x \in S$, то $x = g(x,t)$ для некоторого t. И обратно, если $x = g(x,t)$ для некоторого t, то $U(p,x)$ определена, а значит, определена и $f(x)$.

Мы представили S как множество значений функции от двух натуральных аргументов. Чтобы перейти к функциям одного аргумента, используем вычислимую биекцию $c : N \times N \to N$ и выразим S как $S = g \circ c^{-1}(N)$. **[:|||:]**

Теорема 24

Теорема. *Непустое множество значений вычислимой фукнции является множеством значений всюду определенной вычислимой фукнции.*

Доказательство. Пусть $S = f(\mathbb{N})$ для некоторой вычислимой f. Пусть $f(x) = U(p,x)$ для некоторой у.в.ф. U, для которой существует отладочная функция F.

Пусть g – всюду определенная фукнция $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, определенная следующим образом:

$$g(x,t) = \begin{cases} U(p,x), & F(p,x,t) = 1 \\ a, & \text{иначе} \end{cases}$$

Множество значений g совпадает с S: если $y = g(x,t)$, то $y = a \in S$ или $y = U(p,x) = f(x) \in S$. В другую сторону: пусть $y = f(x) = U(p,x)$. На паре (p,x) фукнция определена, значит существует t, такое что $F(p,x,t) = 1 \Rightarrow y = g(x,t)$. Получили, что множество S представимо в виде множества занчений тотальной функции от двух аргументов. Осталось перейти к функции от одного аргумента, использовав любую вычислимую биекцию.

[:|||:]

Теорема 25

Теорема. *Множество S, являющееся областью определения универсальной фукнции является перечислимым, но неразрешимым множеством.*

Доказательство. Перечислимость. Пусть S – область определения некоторой вычислимой фукнции f. Такая область перечислима. Обозначим через p номер функции в нумерации U. Получим что

$$S = \{x : U(p,x) \text{определена}\}$$

Неразрешимость. Если бы оно было разрешимо, что из алгоритма разрешения получался бы алгоритм разрешения любого перечислимого множества. **[:|||:]**

Теорема 26

TO BE WRITTEN. DEADLINE: 12.03.2017

Теорема 27

Теорема. *Функция вычислима тогда и только тогда, когда ее график перечислим.*

Доказательство. 1) Пусть функция f вычислима. Тогда возможно перечислить ее график через функцию отладки: будем перечислять $\mathbb{N}^3$ и 2) Пусть график функции f перечислим. Тогда алгоритм ее вычисления тривиален: перечисляем график и на каждой выданной паре будем сравнивать вход с первой координатой. Если функция определена, значит она когда-нибудь **[:|||:]**

Теорема 29

Определения:

- **Свойством** называется некоторое подмножество множества F всевозможных вычислимых функций.
- Свойство A называется **нетривиальным**, если $A \neq F$ и $A \neq \varnothing$.

Пусть U — главная универсальная функция.

Теорема. *Теорема Успенского-Райса: для любого нетривиального свойства A множество $\{n \,|\, U(n,x) \in A\}$ неразрешимо.*

Доказательство. Пусть A — нетривиальное свойство, α — нигде не определённая функция. Без ограничения общности предположим, что $\alpha \in A$ (если это не так, рассмотрим $\overline{A}$: A разрешимо тогда и только тогда, когда $\overline{A}$ разрешимо). Пусть $\beta \in \overline{A}$ — некоторая вычислимая функция (такая функция существует, так как A нетривиально). Рассмотрим произвольное перечислимое, но не разрешимое множество K и функцию $V(n, x)$, заданную следующим образом:

$$V(n,x) = \begin{cases} \beta(x) \text{ при } n \in K \\ \alpha(x) \text{ при } n \notin K \end{cases}$$

Данная функция вычисляется алгоритмом, который запускает перечисляющий алгоритм $\mathfrak{A}$ множества K, каждый вывод $\mathfrak{A}$ сравнивает с n и в случае равенства останавливается и возвращает $\beta(x)$ как результат своей работы. При $n \in K$ алгоритм $\mathfrak{A}$ выведет n через конечное число шагов, и вышеописанный алгоритм остановится за конечное число шагов, а при $n \notin K$ вышеописанный алгоритм никогда не остановится, так как условие есго остановки (равенство

некотрого вывода $\mathfrak{A}$ и n) никогда не будет выполнено.
Поскольку U — главная универсальная функция, существует всюду определённая вычислимая функция s такая, что $V(n,x) = U(s(n), x)$ для любых x и n. Предположим, что $\{n \mid U(n, x) \in A\}$ — разрешимое множество. Заметим, что $n \in K \Leftrightarrow U(s(n), x) \notin A$ по определению $V(n, x)$. Если $\{n \mid U(n, x) \in A\}$ разрешимо, то разрешимо и $\{n \mid U(s(n), x) \in A\}$ (поскольку s — всюду определённая вычислимая функция), а следовательно, и K. Однако K — неразрешимое множество. Значит, предположение неверно, и $\{n \mid U(n, x) \in A\}$ неразрешимо для любого нетривиального A. **[:|||:]**

Теорема 30

Пусть U — главная универсальная функция, p — всюду определённая вычислимая функция.

Теорема. *Теорема о неподвижной точке: существует такое t, что $U(t, x) = U(p(t), x)$ при любых x.*

Доказательство. Рассмотрим функцию $a(x) = U(x, x)$. Поскольку U — главная универсальная функция, $U(a(x), y) = V(x, y) = U(s(x), y)$ для любого y, где s — некоторая всюду определённая вычислимая функция. Так как композиция $p \circ s$ — всюду определённая вычислимая функция, существует $C(p, s) = q$ такое, что $U(q, x) = U(p, U(s, x))$ (в данном случае под p и s понимаются U-номера соответствующих функций, то есть $U(p, U(s, x))$ — это то же самое, что и $p(s(x))$).
Докажем, что $s(q)$ является непожвижной точкой для функции p: заметим, что $U(p(s(q)), x) = U(U(q, q), x)$ по определению q. В свою очередь, $U(U(q, q), x) = U(a(q), x) = U(s(q), x)$ по определению $a(x)$. Таким образом, $U(p(s(q)), x) = U(s(q), x)$, что нам и требовалось. **[:|||:]**