Смысл машины Тьюринга

Оказывается, что всякую функцию из $Д^* \to Д^*$, которую можно вычислить по какому-либо алгоритму, можно вычислить на машине Тьюринга. Но об этом мы поговорим чуть позже.
Рассмотрим вначале понятие алгоритма.
В математике есть неопределенные понятия, например такие как натуральные числа. К числу таких понятий относится и алгоритм. Его понятие определяется интуитивно.
Обозначение: ! - означает, что далее стоит определенное слово.
Обозначение: $\simeq$ означает что и справа и слева стоят либо одновременно определенные и равные слова, либо одновременно неопределенные слова.
Рассмотрим произвольный алгоритм: его состав:
1) область возможных исходных данных;
2) область возможных результатов.
Алгоритм преобразует элемент множества 1 в элемент множества 2. Соответственно, в 1 возникает подмножество - $1'$ - область результативности, то есть те элементы для которых есть результат.
Множество результативности описывается так: $\{x|!A(x)\}$
Определение: $f : Д^* \to Д^*$ вычислима, если существует вычисляющий ее алгоритм, то есть $f(x) \simeq \ddot{А}(x)$, где Ä обозначает алгоритм.
Тезис Черча в версии Тьюринга: Любая вычислимая функция $f : Д^* \to Д^*$(Д - алфавит) вычислима на машине Тьюринга.
Будем считать, что вход алгоритма - всегда слово.
Бывают свойства слов, которые алгоритмически определяются. Такие свойства называются разрешимыми.
Определение: $X \subset В^*$, X - разрешимо, если $\exists\ddot{А}$ - алгоритм дающий ответ на вопрос: $x \in X$?(для любого x из $Б^*$)
Например, множество четных чисел разрешимо. Всего разрешимых множеств счетно, поскольку алгоритмов счетно.
Теорема: Пересечение, объединение и дополнение разрешимых множеств разрешимо.
Доказательство: ◄ Доказательство проводится путем построения алгоритма для пересечения, объединения, дополнения из двух алгоритмов для множеств. ►
Определение: Характеристическая функция множества - это функция, значение которой равно 1, если элемент принадлежит множеству, и 0 в противном случае(то есть если элемент принадлежит дополнению).
Определение: Полухарактеристическая функция множества - это функция, значение которой равно 1, если элемент принадлежит множеству, и которая не определена в противном случае(то есть если элемент принадлежит дополнению).
Определение: Множество полуразрешимо, если полухарактеристическая функция вычислима.
Определение: Не более чем счетное множество - это такое множество, которое является множеством членов некоторой последовательности.
Определение: Перечисленное множество - это такое множество, которое является множеством членов некоторой вычислимой последовательности.
Рассмотрим два произвольных перечисленных множества:
Например, множество $\mathbb{N}^2$ - перечислим.
$A = \{a_0, a_1, a_2...\}$
$B = \{b_0, b_1, b_2...\}$
Свойства перечисленных множеств
1) Прямое произведение перечисленных множеств перечислим;
2) Объединение перечисленных множеств перечислим;
3) Пересечение перечисленных множеств перечислим;

Доказательство: ◀ 1) Рассмотрим пары $< a_k, b_l >$. Ясно, что $\mathbb{N}^2 = \{< \xi(n), \eta(n) >\}$ - вычислимое произведение. А множество вида - $\{< a_{\xi(n)}, b_{\eta(n)>}\}$ - это все виды пар.
Отсюда следует перечислялось прямого произведения.
2) Если $A = \emptyset$ или $B = \emptyset$ то все очевидно. Предположим, что A и B - не пусты. Пусть A и B - множество членов вычислимых последовательностей f и g. Пусть h(n) задается так: $h(n) = f(\frac{n}{2})$, если n четно и $h(n) = g(\frac{n-1}{2})$. Эта последовательность вычислима, и её множество значений - это $A \cup B$.
3) Если $A = \emptyset$ или $B = \emptyset$ то все очевидно.
Предположим, что A и B - не пусты. Тогда $\exists c \in A \cap B$. Рассмотрим последовательность $c_n = a_{\xi(n)}$, если $a_{\xi(n)} = b_{\eta(n)}$ и $c_n = c$, если $a_{\xi(n)} \neq b_{\eta(n)}$. Множество значений этой последовательности и есть пересечение. ▶
Имеет место еще одна теорема про перечисленные множества:
Теорема: Прообраз и образ перечислением множества при вычислимой функции перечислены.
Доказательство: ◀ Прообраз перечислением множества A при вычислимой функции f - это проекция пересечения графика f с перечисленным множеством $\mathbb{N} \times A$ на первую координату. Из свойств перечисленных множеств получаем, что прообраз перечислим. ▶
Рассмотрим дополнение к перечисленному множеству - оно не обязательно перечислим. Для приведения примера докажем:
Теорема: Множество разрешимо $\Leftrightarrow$ оно перечислимо и его дополнение перечислимо.
Доказательство: ◀ ($\Rightarrow$) Пусть $S \subset Б^*$ и S - разрешимо.
Если S - пусто, то все ясно. Иначе $\exists s \in S$.
Пусть $Б^* = \{b_0, b_1, ...\}$ - вычислимая последовательность.
Строим $s_n = \begin{cases} b_n, & b_n \in S \\ s, & b_n \notin S \end{cases}$ Множество значений s = S, значит множество перечислимо, а из того, что дополнение разрешимого множества разрешимо следует, что и дополнение перечислимо.
($\Leftarrow$) Если одно из множеств(множество или дополнение) пусто, то все ясно. Пусть оба не пусты. И $S = \{x_0, ..., x_n, ...\}$ и $Б^* \backslash S = \{y_0, ..., y_n, ...\}$. Рассмотрим произвольный элемент $x \in S$. Найдем какому из множеств: S или $Б^* \backslash S$ принадлежит z. Для этого будем выписывать по одному элементу: x_n и y_n. На каком-то шаге мы выпишем и z. Значит для любого z мы можем сказать принадлежит оно S или нет, то есть S - разрешимо. ▶
Теорема: Каждое перечислимое множество является полуразрешимым.
Доказательство: ◀ Пусть R - перечислимое множество. Если R - пусто, то теорема очевидна. Пусть R - не пусто. $Б^* \supset R = \{r_0, ...r_n, ...\}$
Надо построить такую функцию:
1) $x \in R \Rightarrow f(x)$ определена.
2) $x \in Б^* \backslash R \Rightarrow f(x)$ неопределена. Ясно, что искомая функция: f(x)=наименьшее n, такое что $r_n = x$.
Алгоритм ее вычисления таков: берем x и выписываем вычислимую последовательность членов R. Если $x \in R$, то мы до него дойдем на каком-то шаге, если же $x \notin R$ то функция будет не определена. Значит f - полуразрешимо.▶

Определение: Пусть $A \subset X_1 \times X_2 \times ... \times X_n$.
Тогда $\text{пр}_{1,...,i-1,i+1,...n} A = \{< a_1 ... a_{i-1}, a_{i+1}, ... a_n > | \exists a_i :< a_1, ... a_n > \in A\}$
Проекция перечислимого множества перечислима. Проекция разрешимого множества необязательно разрешима, поскольку непонятно, как выяснить существует ли a_i такое, что $< a_1, ... a_n > \in A$. Но эта проекция перечислима.
Определение: Тотальной функцией называется всюду определенная функция.
Заметим(пока без доказательства), что существует вычислимая функция, которую нельзя продолжить до тотальной вычислимой.

Область определения этой функции не разрешима, иначе существовало бы вычислимое тотальное продолжение, которое можно построить так:

$$g(x) = \begin{cases} f(x), & \text{если } \exists f(x), \text{т.е. } x \in D(f); \\ a, & \text{если } \nexists f(x), \text{т.е. } x \notin D(f); \end{cases}$$

Значит область определения этой функции не разрешима.

Рассмотрим произвольный алгоритм Ä. Его область возможных исходных значений: X.

Рассмотрим высказывание: На n-ом шаге или ранее, Ä с применением ко входу X закончит работу с результатом.

Ясно, что есть другой алгоритм по n и x определяющий истинностное значение высказывания.

Обозначим эту высказывательную форму: $\alpha(x, n)$ и рассмотрим $S = \{< x, n > \mid \alpha(x, n) -$верно$\}$.

S разрешимо, как подмножество: $S \subset X \times \mathbb{N}$.

Определение: S называется сигнализирующим множеством Ä.

1) Пусть f - вычислимая функция, S - сигнализирующее множество.

D(f) - это те x, для которых $\exists n$: такое, что не позже чем не n шаге будет получен результат, т.е. $< x, n > \in S$, значит Д$(f) = \text{пр}_1 S$. Поскольку S разрешимо, то **Д(f)**, как проекция S, **перечислимо**.

Отсюда можно сделать вывод, что перечислимые и области определения - это один и тот же класс множеств.

2) Теперь будем исследовать E(f), где f вычислима.

Докажем, что E(f) перечислима. Перечислим Д(f): $\{d_0, d_1, ..., d_n, ...\}$ и возьмем перечисление: $\{f(d_0), f(d_1), ..., f(d_n), ...\}$ - это вычислимая последовательность, поскольку на этих точках функция f определена.

3) Рассмотрим график вычислимой функции. Имеет место следующая теорема.

Теорема о графике: Функция вычислима $\Leftrightarrow$ ее график является перечислимым множеством.

Доказательство: ◄ ($\Rightarrow$) Пусть f вычислима. Если f нигде не определена, то теорема очевидна. Пусть Д$(f) = \{d_0, d_1, ...\}$ - вычислимая последовательность. Тогда график f есть такое множество: $\{< d_0, f(d_0) >, < d_1, f(d_1) >, ..., < d_n, f(d_n) >, ...\}$, т.е. график перечислим.

($\Leftarrow$) Если график пуст, то f нигде не определена, а значит вычислима. Пусть график не пуст. Перечислим его: $\{< x_0, y_0 >, < x_1, y_1 >, ...\}$. Алгоритм вычисления функции f таков: перебирать все n из $\mathbb{N}$ пока не найдем n, такое, что $x_n = x$. На выход подать $f(x_n)$. ►

Итак, следующие свойства M равносильны:

1) M - перечислимо;
2) M - полуразрешимо;
3) M - проекция разрешимого множества;
4) M является Д(f) для некоторой вычислимой f;
5) M является E(f) для некоторой вычислимой f.

Рассмотрим кодирование программ машины Тьюринга.

Пусть d - ленточный алфавит машины Тьюринга. $d = \{a_0; a_1; ...; a_m\}$; $Q = \{q_0, q_1, ..., q_n\}$

Одна команда записывается так: $q_i a_j \to a_k \nabla q_l$.

Кодируется этот алгоритм так: a_j : $\underbrace{a||...|}_{\text{j штрихов}}$ и q_i : $\underbrace{q||...|}_{\text{i штрихов}}$ бланк : a $\underbrace{}_{\text{0 штрихов}}$

Алфавит кодирования: $\Pi = \{|,\ q,\ a,\ \to,\ L,\ R,\ N,\ \underbrace{\downarrow}_{\text{разделительный знак}}\}$

Т.е. любая программа - слово в этом алфавите.

P - все программы $\subset \Pi^*$. Так как P перечислимо, то $P = \{\pi_0, ..., \pi_n, ...\}$

Для произвольной машины Тьюринга нельзя определить функцию, которую она записывает, поскольку мы не знаем рабочий алфавит (а как раз из него и берутся аргументы) машины.

Если же алфавит задан, то функция определяется.
Множество всех программ $P(\subset \Pi^*)$ - разрешимо, поскольку по слову можно определить является оно программой или нет.
Если перечислимое множество бесконечно, то его можно расположить в вычислимую последовательность без повторяющихся членов. Отсюда следует, что между любыми двумя бесконечными перечислимыми множествами существует вычислимая в обе стороны биекция.
Вернемся к P. Поскольку оно разрешимо, то оно перечислимо. $P = \{\pi_0, \pi_1, ..., \pi_n, ...\}$
Обозначение: $Com(X, Y)$ - множество всех вычислимых функций из X в Y.
Рассмотрим функцию: $\Phi : \mathbb{N} \times Б^* \to Б^*$.
Определение: $\Phi(n, x)$ - называется универсальной для $Com(X, Y)$, если
1) Φ вычислима;
2) $\forall f \in Com(Б^*, Б^*) \exists n \in \mathbb{N} : \Phi(n, x) \simeq f(x),\ \forall x$
Заметим, что множество всех вычислимых функций из X в Y счетно, поскольку счетно множество алгоритмов(как слов в алфавите).
Существование универсальной функции для Com(X,Y):
Поскольку Com(X,Y) счетно, то Com(X,Y)=$\{f_0, f_1, ...\}$.
Положим $\Phi(n, x) \simeq f_n(x), \forall n \in \mathbb{N}, \forall x \in X$. Это и есть искомая универсальная функция.

Рассмотрим $\Phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Рассмотрим $f(x) = \Phi(x, x) + 1$. f(x) - вычислимая, значит $\exists m : \Phi(m, x) = f(x)$. Рассмотрим f(m): $\Phi(m, m) = f(m) = \Phi(m, m) + 1$. Получается противоречие, поскольку изначально было предположено, что $\Phi(m, m)$ определено, однако, как оказывается это не так. Имеет место:
Теорема: Существует вычислимая функция, которая не продолжается до тотальной вычислимой функции.
Доказательство: ◀ Предположим, что φ вычислима, и продолжается до ψ - тотальной, вычислимой функции. Тогда $\exists j\ \psi(x) \simeq \Phi(j, x)$.
Поскольку $\psi(j)$ - определено, то и $\Phi(j, j)$ - определено, значит $\varphi(j)$ - определено(поскольку $\varphi(x) \simeq \Phi(x, x) + 1$), и верно, что $\psi(j) = \varphi(j)$, поскольку ψ - продолжение φ, значит $\Phi(j, j) = \psi(j) = \varphi(j) = \Phi(j, j)$+1. Получаем противоречие, значит функция не продолжается до тотальной вычислимой. ▶
Приведем пример перечислимого неразрешимого множества при помощи только что доказанной теоремы:
Теорема: Существует перечислимое неразрешимое множество (или: существует перечислимое множество с неперечислимым дополнением).
Доказательство: ◀ Рассмотрим вычислимую функцию f(x), не имеющую всюду определенного вычислимого продолжения и возьмем ее область определения: A. По доказанному выше, A - перечислимо. Предположим, что A - разрешимо. Рассмотрим функцию $\overline{f}(x)$= $\begin{cases} f(x), & \text{если } x \in A; \\ 0, & \text{если } x \notin A. \end{cases}$
Эта функция является всюду определенным вычислимым продолжением f(x). Противоречие. ▶