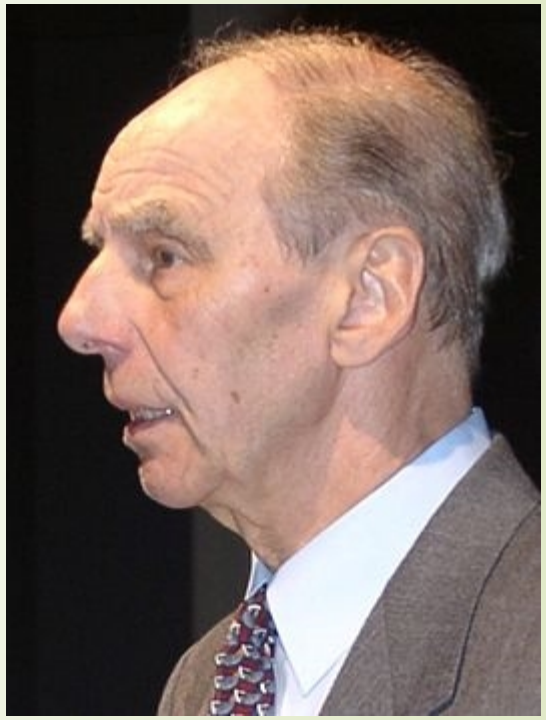
Юрис Хартманис

Петрозаводский государственный университет
Ильин Даниил Леонидович
daniil.ilin@gmail.com
2017

Juris Hartmanis

- Дата рождения: 5.07.1928
- Родился в семье генерала латвийской армии Мартиньша Хартманиса
- Степень магистра по физике Марбургского университета имени Филиппа (1949 г.)
- Степень магистра по прикладной математике (университет Миссури в Канзас-сити 1951 г.)
- Доктор философии по математике (Калифорнийский технологический институт 1955 г.)
- Преподавал, потом устроился в исследовательскую лабораторию General Electric (1958 г.)
- Основал факультет информатики в Корнеллском университете (1965 г.)



Теория сложности вычисления

- Вычислительная сложность — понятие в информатике и теории алгоритмов, обозначающее функцию зависимости объёма работы, которая выполняется некоторым алгоритмом, от размера входных данных. Раздел, изучающий вычислительную сложность, называется теорией сложности вычислений.
- Как изменится время исполнения и объём занятой памяти в зависимости от размера входа?
- Классы сложности

Теорема об иерархии по времени

- Пусть f и g — две вычислимые конструируемые по времени функции, и g(n) = ω(f(n) log f(n)). Тогда класс DTIME(f(n)) строго вложен в класс DTIME(g(n)).
- Классом DTIME(*f*(*n*)) называется множество языков, для которых существует машина Тьюринга такая, что она всегда останавливается, и время ее работы не превосходит *f*(*n*), где *n* — длина входа.
- Доказывается при помощи диагонального метода – строится язык, который принадлежит классу DTIME(g(n)), но не принадлежит классу DTIME(f(n)).

Диагональный метод Кантора

- Теорема Кантора - Обозначим через X множество всех действительных чисел, или, что то же, всех точек единичного отрезка [0,1]. Множество X – несчетно.
- Для доказательства допустим, что X счетно. Это, по определению, означает, что все его элементы можно занумеровать с помощью обычных конечных натуральных чисел. Построим последовательность таких двоичных чисел. Далее, строится новое число по следующему правилу: первая цифра числа не равна первой цифре первого числа последовательности, вторая цифра числа не равна второй цифре второго числа последовательности и т.д., т.е. по диагонали.
- Таким образом мы получаем новое число, а значит утверждение, что X – счетно – неверно.

Доказательство теоремы об иерархии по времени

- Через C(x) обозначим машину $M_f(x, x)$, то есть на вход симулятора подаются два одинаковых слова. Через D(x) обозначим инверсию машины C(x), то есть машину, работающую так же, но выдающую противоположный ответ (если C допускает слово x, то D отвергает x, и наоборот). Через L обозначим язык, распознаваемый машиной D («диагонализирующая» машина), т.е. L=L(D). Покажем, что это и есть требуемый язык. Так как функции конструируемы по времени, то D работает время O(g(n)), а значит, язык L принадлежит классу DTIME(g(n)). С другой стороны, для любой машины M, распознающей язык из класса DTIME(f(n)), по построению машины D справедливо неравенство $M(M) \neq D(M)$ (Через M(M) обозначим множество всех слов $x \in A^*$, допускаемых машиной Тьюринга M). А это означает, что язык L отличается от любого языка из класса DTIME(f(n)): от языка, распознаваемого машиной M язык L отличается в строке, представляющей собой закодированное представление машины M. Поэтому, L не принадлежит классу DTIME(f(n)).

Премия Тьюринга

- Hartmanis J., Stearns R.E. [1965] On the computational complexity of algorithms Trans. Amer. Math. Soc., 117, № 5, 285-306 (Русский перевод в Кибер. сборнике., 1967, 4.) 66.02.67
- Доказательство теоремы об иерархии по времени
- Представлено множество классов сложности DTIME

Лауреат премии “Интернет-математика”

- Сатоси Накамото – создатель протокола криптовалюты биткойн и создатель первого ПО Bitcoin v0.1 (09.01.2009), в котором этот протокол был реализован
- Криптовалюта — вид цифровой валюты, эмиссия и учёт которой основаны на криптографических методах, например методе защиты Proof-of-work и асимметричному шифрованию, а функционирование системы происходит децентрализовано в распределённой компьютерной сети.
- Bitcoin — децентрализованная электронная криптовалюта. Под словом "децентрализованная" понимается, что Bitcoin не имеет каких-либо централизованных серверов для выпуска новых монет, обработки транзакций или хранения средств.

Законность криптовалюты

- Законопроект о запрете биткоинов – январь 2014 – не принят
- Центробанк РФ рассматривает возможность признания Биткоина – июнь 2015
- Минфин подготовил поправки в Уголовный Кодекс, предлагая ввести наказание за выпуск денежных суррогатов – март 2016
- Э.Набиуллина, председатель Банка России высказалась против легализации
- А.Кудрин поддержал инициативу – сентябрь 2017
- В.Путин положительно отозвался о возможности легализации криптовалюты – октябрь 2017

Криптовалюта не запрещена территории РФ.

Источники

- Faculty Biographies [Электронный ресурс] Cornell CIS Computer Science: сайт Корнелльского университета URL: http://www.cs.cornell.edu/annual_report/00-01/bios.htm#hartmanis
- 15 Unusual Facts & Theories About Mysterious Bitcoin Founder Satoshi Nakamoto [Электронный ресурс] Inc. : американский ежемесячный деловой журнал URL: https://www.inc.com/larry-kim/15-unusual-facts-amp-theories-about-mysterious-b.html
- JURIS HARTMANIS [Электронный ресурс] A.M. Turing Award: сайт лауреатов премии Тьюринга URL:http://amturing.acm.org/award_winners/hartmanis_1059260.cfm
- М.Г. Агидеев Введение в теорию сложности [Электронный ресурс]: Ростов-на-Дону 2004 г. URL: http://www.ict.edu.ru/ft/004803/Comp.pdf