МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2012
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2012
Proceedings of the Forty First Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 9–12, 2012

АЛАН ТЮРИНГ – ЕНИГМАТИЧНИЯТ ГЕНИЙ НА ИНФОРМАЦИОННАТА ЕРА

Радослав Павлов

През 1936 г. Алан Тюринг публикува статията *"On Computable Numbers, with an Application to the Entscheidungsproblem"*, в която доказва за първи път изчислителната неразрешимост на проблем – известния Entscheidungsproblem на Давид Хилберт. Значението на тази статия е огромно не само за математиката, но и за развитието на компютърната техника и наука. В нея той представя най-общ абстрактен формален модел на изчислителен процес, наречен по-късно машина на Тюринг, с който определя и границите на изчислимостта. Представената също там универсална машина на Тюринг може да се разглежда като идеализиран модел на логическото устройство на съвременни компютри.

Докладът е посветен на 100-годишнината от рождението на Алан Тюринг.

(1912–1954)

През 1936 г. 24-годишният английски математик Алан Тюринг публикува статията *"On Computable Numbers, with an Application to the Entscheidungsproblem"*. Тази статия изиграва изключително важна повратна роля не само в математиката, но и за възникването и развитието на съвременните компютри и на науката за тях. Работейки над проблем на Хилберт, той създава модел на изчислителен процес, в който всеки алгоритъм се разлага на поредица от елементарни стъпки, които могат да се изпълняват механически, т.е. без творческа намеса. Този най-общ абстрактен модел, наречен по-късно машина на Тюринг, определя и границите на изчислимостта и може да се справи с кое да е изчисление за достатъчно дълъг, но краен срок от време. По своето логическо устройство всеки съвременен компютър не е нищо друго, освен една от машините на Тюринг, наречена от него универсална. Машините на Тюринг създават възможността самото понятие „изчислителен процес“ или „алгоритъм“ да се изследва с математически средства, което има фундаментално значение за развитието на изчислителните науки.

Машината на Тюринг представлява идеализирано компютърно устройство с неограничена външна памет, организирана така, че всеки елемент на запомнена информация да бъде потенциално достъпен за прочитане и замяна. При нея изчислителният процес е максимално разчленен на елементарни „механично“ изпълними операции, управлявани от крайна програма, за да се получи стандартна, проста и същевременно най-обща схема, чрез която да може да се моделира произволен изчислителен процес. На неформално ниво най-често машината на Тюринг се описва като устройство, съставено от такива атрибути като лента и придвижващо се по лентата четящо и пишещо управляващо устройство, описание, въведено от самия Тюринг. В съответствие с това една машина на Тюринг се състои от управляващо устройство, което във всеки момент от време се намира в едно от краен брой вътрешни състояния, и лента, която е крайна, но може да бъде продължавана неограничено и в двете посоки. Лентата е разделена на клетки и във всяка клетка е записан точно един символ от дадена лентова азбука. Част от лентовите символи образуват входната азбука, чрез която се задава върху лентата входната информация. Един от лентовите символи, който не е входен, е фиксиран и когато той е записан в дадена клетка, казва се, че тази клетка е празна. Клетките, които се добавят при продължаването на лентата, са винаги празни. Управляващото устройство във всеки момент от време може да прочете символа, записан в една от клетките на лентата, да запише на негово място нов лентов символ и да се придвижи с една клетка наляво или надясно. Едно от вътрешните състояния е фиксирано и се нарича начално, а част от вътрешните състояния се наричат заключителни.

Машината на Тюринг работи в дискретни, мигновенни стъпки, наречени тактове. Започва работа в начално състояние, на лентата е записана дума от входни символи, а управляващото устройство се намира на някакво определено място на лентата, например върху най-левия входен символ. При всеки следващ такт управлявавещото устройство, в зависимост от вътрешното си състояние и прочетения лентов символ, определя в какво ново вътрешно състояние да премине, кой символ да запише в клетката на прочетения символ и коя нова клетка да прочете – тази, която е непосредствено отдясно на прочетената, или тази, която е непосредствено отляво. Движението наляво или надясно е винаги възможно, тъй като при необходимост към лентата се прибавя празна клетка. Машината на Тюринг спира работа, ако в управляващото устройство няма инструкция как да продължи, но може да работи и неограничено дълго. В случай, че спре, резултат от работата е това дали е спряла в заключително състояние (ако тя работи като разпознавател) или какво е записано на лентата (ако работи като преобразувател).

Формално една машина на Тюринг се дефинира като наредена седморка: $\langle K, V, W, F, s, B, Z \rangle$ с

– множество K на вътрешните състояния с подмножество Z на заключителните състояния;
– множество W на лентовите символи с подмножество V на входните символи;
– начално вътрешно състояние s;
– лентов символ B за празната клетка, който не е входен;
– функция на преходите F с дефиниционна област $D(F) \subseteq K \times W$ и област на стойностите $R(F) \subseteq K \times W \times \{R, L\}$, където R и L не са нито състояния, нито лентови символи;

Конфигурация на дадена машина на Тюринг се нарича наредената тройка $\langle A, s, aC \rangle$, където $s \in K$, a е лентов символ, A и C са думи от лентови символи и може да се интерпретира неформално като това какво е записано на лентата (AaC), в какво състояние (s) е управляващото устройство и коя клетка (a) се прочита.

Работата на машината на Тюринг се задава като прехода от една конфигурация към друга, определени от функцията на преходите. Има различни начини да се представя функцията на преходите – таблично, чрез диаграма на преходите или като списък от наредени петорки от вида $\langle s, S_1, S_2, D, q \rangle$, за $F(s, S_1) = \langle q, S_2, D \rangle$, където s, q са състояния, S_1, S_2 – лентови символи, а D е R или L.

Машините на Тюринг могат да се използват и като преобразуватели, които за определен клас целочислени функции намират по дадени стойности на аргументите стойността на функцията. Функциите, за които такава машина съществува, се наричат изчислими по Тюринг функции или още – частично рекурсивни. Ако има такава машина на Тюринг, изчисляваща стойностите на функцията, която да спира след краен брой стъпки за всички допустими стойности на аргументите, такава функция се нарича общорекурсивна.

Да вземем, например, функцията $f(x, y) = x+y$ и нека m и n са цели положителни числа. Прието е входната дума за машината да представлява унарния запис на числата m и n, отделени с някакъв друг символ, например 0:

$$\underbrace{11\ldots1}_{m}0\underbrace{11\ldots1}_{n}$$

Резултат от работата на съответната за $f(x, y)$ машина на Тюринг представлява записаната върху лентата дума от единица, когато машината спре. Следната машина на Тюринг M изчислява стойностите на функцията $f(x, y)$ за цели положителни числа:

$$M = (\{s_0, s_1, s_2\}, \{0, 1\}, \{0, 1, B\}, F, s_0, B, \{s_2\})$$

с функция на преходите

$$F(s_0, 1) = (s_0, 1, R), \quad F(s_1, 1) = (s_1, 1, R), \quad F(s_2, 1) = (s_2, B, R),$$

$$F(s_0, 0) = (s_1, 1, R), \quad F(s_1, B) = (s_2, B, L).$$

Машината M действа по следния прост начин: движи се надясно през първия блок от единици, докато открие нулата, превръща я в единица и продължава надясно, докато открие края на следващия блок от единици. След това изтрива последната единица, минава надясно и спира. Ясно е, че на лентата ще бъде записан блок от $m + n$ единици.

Машините на Тюринг определят и границите на ефективната изчислимост. Формалното понятие, което Тюринг предлага е „изчислимост чрез машина на Тюринг“.

Той аргументира твърдението, че ако въобще съществува някакъв ефективен метод за получаване на стойностите на математическа функция, тази функция се изчислява и чрез машина на Тюринг. Обратно, всяка изчислима по Тюринг функция се пресмята посредством определена „механична“ процедура, зададена от машина на Тюринг, която напълно съответства на интуитивната ни представа за ефективен метод или алгоритъм. Тюринг изказва следната хипотеза: класът на ефективно (алгоритмично) изчислимите функции съвпада с класа на изчислимите по Тюринг функции.

Това твърдение е известно като „тезис на Тюринг“, „тезис на Тюринг-Чърч“, „тезис на Чърч“, тъй като Алонзо Чърч, независимо от Тюринг, през 1936 г. изказва подобна теза за разработения от него формализъм на ламбда-определимите функции.

Освен Алан Тюринг и Алонзо Чърч, редица математици разработват други формализми за понятието „ефективно (алгоритмично) изчислима функция“. Всички те могат да бъдат моделирани чрез машини на Тюринг и се свеждат до тях.

Опитите да бъде опроверган тезисът на Тюринг-Чърч (например Калмар (1959), Менделсон (1963) и др.) са неуспешни. Макар и във формата на естественонаучна хипотеза тезисът на Тюринг-Чърч е общоприет и класът на изчислимите по Тюринг функции определя границите на ефективната изчислимост.

В своята статия Алан Тюринг описва и машина U, която може да изпълнява работата на всяка отделна машина на Тюринг. Тази машина, наречена универсална, може по зададени кодирани описания на функцията на преходите на произволна машина M и на лентова дума A за M да извършва изчислителния процес, породен от A за M и да спре (в заключително състояние) тогава и само тогава, когато M спира (в заключително състояние). В случай, че спре, U съдържа върху лентата си кодирано описание на крайната конфигурация, в която M би спряла.

Както отбелязва Тюринг, всяка машина на Тюринг може да бъде кодирана на лентата с редица от 0 и 1, тъй като тя се определя еднозначно от функцията на преходите ѝ, чиято таблица е крайна. Същото може да се направи и с всяка лентова дума, тъй като лентовата азбука е също крайна.

Универсалната машина на Тюринг U задава на лентата си три зони – буферна зона, зона за кодираното описание на M и зона за кодираното описание на лентовата дума за M. Буферната зона се използва за записване на кодовете на текущото вътрешно състояние на M и на прочетения лентов символ при всеки такт на M. Изчислителният процес на U, моделиращ работата на M върху лентовата ѝ дума се извършва на фази, които съответстват на преходите от една конфигурация към друга в моделирания процес.

Универсалната машина на Тюринг може да се разглежда като предшественик и идеализиран математически модел на всеки универсален компютър. Подобно на нея компютърът започва работа с програма, написана на някакъв език за програмиране, и входни данни, преработва програмата и данните на машинен език и след това я изпълнява.

Универсалната машина на Тюринг може да имитира работата на всяка друга машина на Тюринг, докато реалният универсален компютър има ограничени възможности за реализация.

Да разгледаме и конкретната задача, повод за написването на тази забележителна статия, така наречения "Entscheidungsproblem" – проблема за разрешимост на Давид Хилберт.

През 1901 г. на Международния математически конгрес в Париж Давид Хилберт представя списък на нерешени математически проблеми. На второ място в този списък е проблемът за доказателство на непротиворечивостта на системата от аксиоми на аритметиката. По-късно Хилберт дава по-обща формулировка, известна като Entscheidungsproblem – да се намери общ метод за определяне на изпълнимостта (истинността) на дадено твърдение, формулирано на езика на формалната логика. Положителен отговор би означавал свеждане на математиката до механични пресмятания. Алан Тюринг се захваща с тази задача и изследвайки понятието „изчислимост" показва, че този проблем на Хилберт е неразрешим.

Първия съкрушителен удар на програмата на Хилберт нанася австрийският математик Курт Гьодел. През 1931 г. той доказва, че всяка непротиворечива система от съждения на формалната логика, която е достатъчно богата, за да могат на нейния език да се формулират твърденията на теорията на числата, трябва да съдържа верни твърдения, които са недоказуеми. Следователно не може да съществува общ метод, определящ дали произволно математическо твърдение е вярно или невярно. Заменяйки понятието истинност с понятието доказуемост, проблемът на Хилберт приема следния вид: съществува ли общ метод, чрез който, изхождайки от множеството логически аксиоми, да се доказват всички верни логически твърдения.

А. Тюринг и А. Чърч, едновременно и независимо, през 1936 г. опровергават тази хипотеза. Алонзо Чърч намира логическа формула, която в неговата система на ламбда-определимите функции е недоказуема.

Тюринг създава прост и точен модел на процеса на изчислимост – машината на Тюринг. Като използваме кодираните им описания, можем да номерираме машините на Тюринг по следния начин: подреждаме кодираните описания по тяхната дължина, а кодираните описания с равни дължини подреждаме по големината на двоичното число, което те представят. Получаваме списъка:

$$M_1, M_2, M_3, \ldots, M_n, \ldots,$$

в който се среща всяка машина на Тюринг, която може да бъде описана в рамките на основния модел. По даден номер i може да се намери M_i, а по произволна машина на Тюринг M да се намери неин номер j.

Следователно, множеството на всички изчислими по Тюринг функции е изброимо, т.е. има една и съща мощност с множеството на естествените числа. Същевременно, следвайки диагоналния метод на Георг Кантор, лесно се вижда, че множеството на целочислените функции е неизброимо, т.е. не всички целочислени функции са изчислими.

През 60-те години машините на Тюринг намират основно приложение като модел за оценка на изчислителните сложности. През 1965 г. Ю. Хартманис и Р. Стирнс използват апарата на машините на Тюринг за определяне точните граници на изчислителната сложност, като за това се използва количеството тактове (времева сложност) или дължината на използваната лента (пространствена сложност) в зависимост от размера на задачата. Съвременната теория на сложността на изчисленията е една изключително развита област от основите на информатиката.

ЛИТЕРАТУРА

[1] A. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proc. London Maths. Soc.*, ser. 2, **42** (1936), 230–265.
[2] A. Turing. Collected Works, Volume 1: Mechanical Intelligence (ed. D. C. Ince). Amsterdam, North-Holland, 1992.
[3] A. Turing. Collected Works, Volume 2: Morphogenesis (ed. P. T. Saunders). Amsterdam, North-Holland, 1992.
[4] A. Turing. Collected Works, Volume 3: Pure Mathematics (ed. J. L. Britton). Amsterdam, North-Holland, 1992.
[5] A. Turing. Collected Works, Volume 4: Mathematical Logic (eds R. O. Gandy, C. E. M. Yates). Amsterdam, North-Holland, 2001.
[6] J. Hartmanis, R. E. Stearns. On the computational complexity of algorithms. *Trans. Amer. Math. Soc.*, **117** (1965), 285–306
[7] J. Hopcroft. Turing machines. Scientific American, May 1984, vol 250, No 5.
[8] Й. Денев, Я. Деметрович, Р. Павлов. Дискретна математика. Изд. Наука и изкуство, 1984.
[9] Р. Павлов. Математическа лингвистика. Изд. Народна просвета, 1982.

Радослав Павлов
Институт по математика и информатика
Българска академия на науките
ул. Акад. Г. Бончев, бл. 8
1113 София
e-mail: radko@cc.bas.bg

ALAN TURING – THE ENIGMATIC GENIUS OF THE INFORMATION AGE

Radoslav Pavlov

In 1936 Alan Turing published the famous paper "On Computable Numbers, with an Application to the Eintscheidungsproblem", in which for the first time proved a computational unsolvability of the well-known Hilbert's problem. The importance of this paper is enormous not only for the mathematics, but also for the computer science foundations and the design of real computers. In this paper Turing presents a general abstract model of computational process, called later "Turing Machine", by which he determines the limits of computability. The proposed there "Universal Turing Machine" may be regarded as an idealized model of the logical computer architecture.

This paper is dedicated to the centenary of Alan Turing.