

Teoretický základ algoritmizace

prof. RNDr. Miroslav Vlček, DrSc.

vlcek@fd.cvut.cz

18. října 2007

Matematické modely počítačů

Již v roce 1936 se

Alan Turing
Alonso Church
Kurt Gödel

zabývali teoretickými základy, na nichž by se dala moderní počítačová věda definovat.

Nezávisle na sobě hledali univerzální model, který by z hlediska funkce bez ohledu na fyzikální vlastnosti popsal chování libovolného výpočtu - algoritmu.

Nejčastěji zmiňovaným řešením se stal model Alana Turinga, který byl založen na matematické abstrakci výpočetního stroje, jenž se označuje jako **Turingův stroj**.

Klasický Turingův stroj



Motivací pro Turingův stroj se stal v roce 1900 tzv. Entscheidungsproblem.

Německý matematik David Hilbert formuloval problém, ve kterém se ptal, zda existuje mechanický proces, kterým je možno rozhodnout o pravdivosti libovolného matematického teorému nebo výroku.

Hilbert se chtěl přesvědčit, zda je například možné vyjádřit kroky matematického důkazu spíše posloupností symbolů, než složitým matematickým aparátem.

Toho se chopil Turing a navrhl stroj, který měl simulovat postup matematika při vytváření důkazu.

Klasický Turingův stroj - cont.

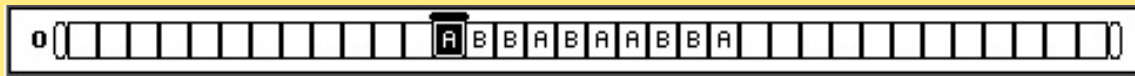
Turingův stroj:

- práce matematika
 - nekonečná tabule (pro psaní i čtení)
 - mozek (řídící jednotka)

Formalizace Turingova stroje

- místo tabule oboustranně nekonečná páska
- místo křídly čtecí a zapisovací hlava, kterou lze posuvat
- místo mozku konečná řídící jednotka

Klasický Turingův stroj - cont.



Takový stroj měl několik základních vlastností:

- musel nahradit složitou symboliku matematických kroků. V takovém případě šlo každou konečnou množinu symbolů nahradit pouze dvěma symboly (jako je 0 a 1) a prázdnou mezerou, která by oba symboly oddělovala.
- podobně jako si matematik zapisuje poznámky na papír, má Turingův stroj k zápisu nekonečnou pásku skládající se z buněk, do/ze kterých se symbol zapisuje/čte.
- nad touto páskou je možné provádět za pomoci čtecí hlavy operace čtení, zápisu a posunu pásky (read, write, shiftright, shiftleft).

Klasický Turingův stroj - cont.

- protože je možné symboly číst, zapisovat nebo se posunovat po pásce, je pro Turingův stroj důležitý vnitřní stav, ve kterém operaci čtení provádíme (čtený symbol a stav tak určují další akci a přechod do dalšího stavu).

Protože se chování tohoto stroje vyvíjí podle tabulky přechodů, můžeme říci, že každý následující stav lze jednoznačně určit na základě čteného symbolu a aktuálního stavu.

Jeho chování je proto *deterministické*.

Klasický Turingův stroj - definice

Turingovým strojem nazýváme pětici

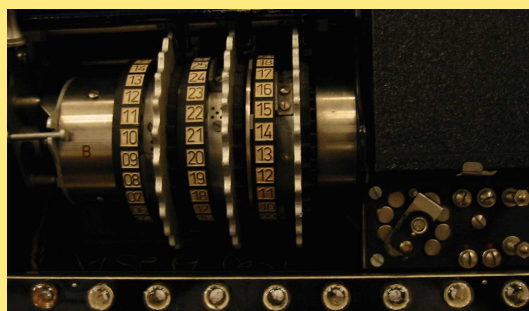
$T \equiv \{Q, X, \delta, q_0, F\}$, kde

- Q neprázdná konečná množina stavů
- X neprázdná konečná množina symbolů, obsahuje symbol ϵ pro prázdné políčko
- δ přechodová funkce $\delta : (Q - F) \times X \rightarrow Q \times X \times \{-1, 0, 1\}$, popisuje změnu stavu, zápis na pásku a posun hlavy
- $q_0 \in Q$ počáteční stav
- $F \subset Q$ množina koncových stavů

Klasický Turingův stroj - definice

1. Výpočet začíná ve stavu $q_0 \in Q$
2. V každém taktu dojde
 - ke změně stavu
 - k přepisu políčka na pásce
 - k posunu hlavy
3. Výpočet končí, když není definována žádná instrukce

Přestože moderní technologie nevídaně od 30.let pokročily, Turingův model můžeme k popisu chování počítačů použít bez úprav i dnes.



Enigma a její vnitřní kódovací válce



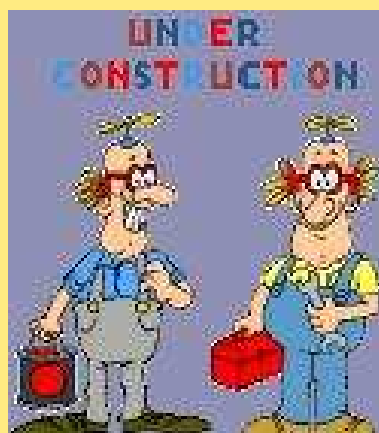
Sítě počítačů

Na základě těchto výsledků dokázal Kurt Gödel, že odpověď na počáteční Hilbertovu otázku je záporná. *"V jakémkoli dostatečně bohatém matematickém systému (jako je např. aritmetika) se dají odvodit výroky jejichž pravdivost nelze pomocí prostředků tohoto systému ani dokázat ani vyvrátit."*



Kurt Gödel 1906 - 1978

Neexistuje mechanický stroj, který by rozhodl pravdivost nebo nepravdivost libovolného matematického výroku.



Děkuji za pozornost