Elementy Teorii Obliczeń

Wykład 2

dr Andrzej Zbrzezny

Instytut Matematyki i Informatyki
Akademia Jana Długosza w Częstochowie

10 stycznia 2009

Maszyna Turinga – uwagi wstępne

- Maszyna Turinga (1936 r.) to jedno z najpiękniejszych i najbardziej intrygujących odkryć 20 wieku. Odkrycie to stworzyło podstawy dla rozwoju informatyki teoretycznej.
- Maszyna Turinga jest prostym ale użytecznym modelem obliczeń (modelem komputerów) wystarczająco ogólnym, aby reprezentować dowolny program komputerowy.
- Z powodu prostego opisu i działania maszyna Turinga poddaje się matematycznym rozważaniom, które doprowadziły do lepszego zrozumienia istoty obliczeń oraz komputerów.
- Jednym z najważniejszych odkryć teorii obliczeń jest fakt mówiący, że istnieją problemy obliczeniowe, które nie mogą zostać rozwiązane na żadnym komputerze, niezależnie od ilości dostępnej pamięci i czasu.

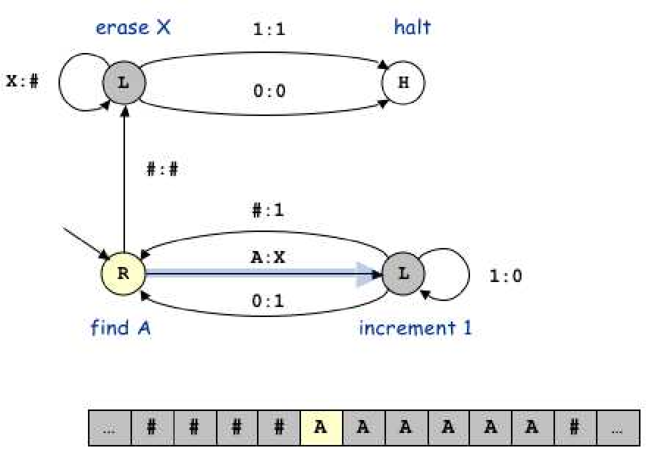
Maszyna Turinga – komponenty

- Potencjalnie nieskończona taśma, na której umieszcza się dane wejściowe, wyniki pośrednie oraz wyniki końcowe.
  - Taśma podzielona jest na komórki.
  - W każdej z komórek znajduje się w danym momencie jeden z symboli skończonego alfabetu.
- Głowica czytająco-pisząca, która w danym momencie znajduje się nad jedną komórką taśmy zwaną komórką aktywną.
  - W każdym kroku głowica czyta symbol z aktywnej komórki i albo pozostawia go bez zmiany albo zapisuje w komórce aktywnej inny symbol.
  - Każdy krok kończy się zmianą stanu oraz przesunięciem głowicy w lewo lub w prawo.

Maszyna Turinga – komponenty

- Jednostka sterująca w postaci diagramu przejść pomiędzy stanami.
  - W zależności od bieżącego stanu oraz symbolu znajdujacego się w aktywnej komórce maszyna Turinga zapisuje na taśmie jednoznacznie określony symbol oraz przechodzi do jednoznacznie określonego stanu.
  - Każda tranzycja wiąże dwa stany (nazwijmy je t oraz s) i jest etykietowana parą symboli (nazwijmy je A oraz X). Oznacza to, że jeżeli maszyna Turinga znajduje się w stanie t a w aktywnej komórce znajduje się symbol A, to w wyniku wykonania tej tranzycji maszyna wpisuje do aktywnej komórki symbol X i przechodzi do stanu t.
  - Każdy stan etykietowany jest jednym z pięciu oznaczeń: L (left), R (right), Y (yes), N (no) lub H (halt).
  - Po wykonania przejścia do stanu t maszyna Turinga w zależności od etykiet tego stanu albo przesuwa głowicę (w lewo lub w prawo) albo zatrzymuje się.

Example (Zamiana liczby z postaci unarnej na binarną)



Działanie maszyny Turinga

- Maszyna Turinga rozpoczyna pracę w wyróżnionym stanie nazywanym stanem początkowym; głowica maszyny Turinga znajduje się nad wyróżnioną komórką nazywaną komórką początkową.
- Dla każdej pary $(stan, symbol)$ istnieje co najwyżej jedna tranzycja związana z tą parą; jeżeli takiej tranzycji nie ma, to maszyna Turinga nie zmienia stanu i nie zmienia symbolu w aktywnej komórce.
- Każdy krok działania maszyny Turinga przebiega jak następuje:
  - czyta symbol z aktywnej komórki
  - szuka tranzycji związanej z bieżącym stanem i z przeczytanym symbolem
  - zmienia symbol w bieżącej komórce
  - zmienia stan zgodnie z tranzycją
  - przesuwa głowicę w lewo lub w prawo lub zatrzymuje się

Działanie maszyny Turinga

- Kroki maszyny Turinga powtarzane są dopóty, dopóki nie znajdzie się ona w stanie etykietowanym przez:
  - H (zatrzymanie),
  - Y (akceptacja) lub
  - N (odrzucenie).
- Jest możliwe, że maszyna Turinga nigdy się nie zatrzyma.
- Założenie o potencjalnie nieskończonej taśmie oznacza, że maszyna Turinga jest modelem obliczeń a nie komputerów.

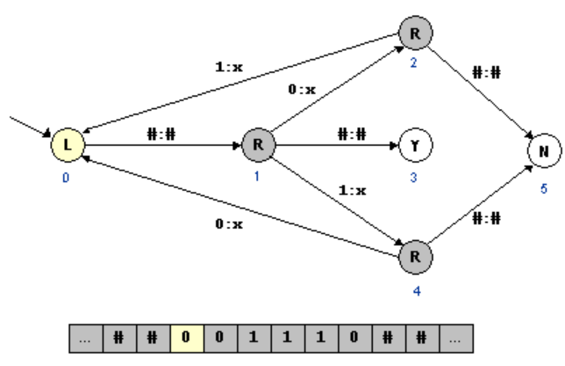
Example (Symulator maszyny Turinga)

- Program `turing.jar`

Uniwersalność

- Na potrzeby teorii obliczeń możemy zdefiniować algorytm jako maszynę Turinga. W tym sensie maszyny Turinga odpowiadają programom komputerowym.
- Uniwersalna Maszyna Turinga (UTM) to specyficzna maszyna Turinga potrafiąca symulować działanie dowolnej innej maszyny Turinga (także samej siebie!).
- UTM pozwala odpowiadać na pytania dotyczące innych TM (także samej siebie!).
- Pierwszą UTM opisał Alan Turing. Istnienie UTM oznacza, że istnieje TM, która potrafi wykonać dowolny algorytm.
- Kluczowa idea polega na sposobie zakodowania dowolnej TM przy pomocy słowa nad skończonym alfabetem.

Kodowanie maszyny Turinga na przykładzie



Kodowanie stanów:

$0L$, $1R$, $2R$, $3Y$, $4R$, $5N$

Kodowanie tranzycji:

$01\#\#$, $201x$, $400x$, $120x$, $13\#\#$, $141x$, $25\#\#$, $45\#\#$

Kodowanie maszyny Turinga

- Aby otrzymać kodowanie konkretnej maszyny Turinga konkatenujemy słowa kodujące stany oraz słowa kodujące tranzycje w słowo nad alfabetem $\{0, 1, 2, 3, 4, 5, x, \#\}$:

  $$0L1R2R3Y4R5N01\#\#201x...45\#\#$$

  i zapisujemy je na taśmie UMT. Po tym słowie umieszczamy słowo nad alfabetem $\{0, 1\}$ będące słowem wejściowym dla zakodowanej TM oddzielając je nowym symbolem.
- Do tego słowa można również dołączyć stan początkowy oraz początkową pozycję głowicy.
- UTM jako wejście otrzymuje kodowanie konkretnej TM oraz początkową zawartość taśmy tej TM.

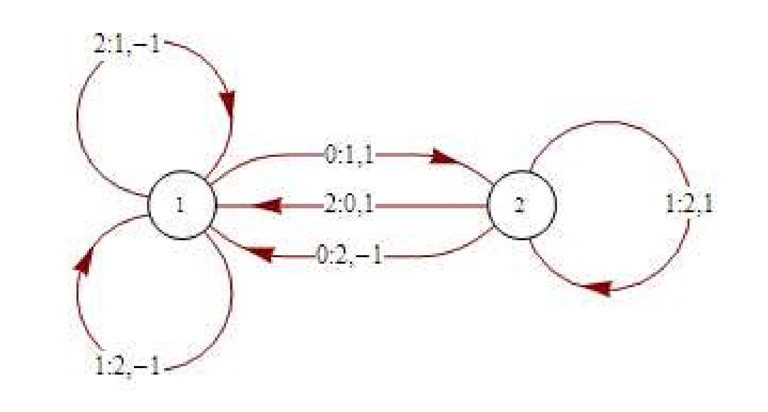
Uwagi na temat istniejących UTM

- Pierwszą UTM opisał Alan Turing w swojej pracy z 1937 roku: "On Computable Numbers, with an Application to the Entscheidungsproblem."
- W 1962 roku M. Minsky odkrył siedmiostanową UTM nad czteroznakowym alfabetem. Z niej można otrzymać UTM nad dwuznakowym alfabetem, ale wymaga to 43 stanów.
- Inne UTM zostały odkryte w 1996 roku przez Rogozhina. Oznaczane są parami liczb (m, n), gdzie m to liczba stanów a n to ilość znaków alfabetu. Są to maszyny: $(24, 2)$, (10, 3), (7, 4), (5, 5), (4, 6), (3, 10) oraz $(2, 18)$.
- W 2002 roku Wolfram odkrył UTM typu $(2, 5)$.
- Uważano, że cztery TM typu $(2, 4)$ oraz czternaście maszyn typu $(2, 3)$ (wszystkie odkryte przez Wolframa) są prawdopodobnie UTM, ale potrafiono tego udowodnić.

Najmniejsza Uniwersalna Maszyna Turinga

- 24 października 2007 roku 20-letni brytyjczyk Alex Smith, student uniwersytetu w Birmingham, zgłosił dowód twierdzenia mówiącego, że zaproponowana przez Wolframa dwustanowa maszyna Turinga używająca tylko trzech symboli jest uniwersalną maszyną Turinga.
- Za to odkrycie Alex Smith otrzymał wcześniej wyznaczoną nagrodę w wysokości $25'000$ dolarów.
- Rozważana maszyna ma w numeracji Wolframa numer $596'440$.
- Istnieje $(2 * 3 * 2 + 1)^{(2*3)} = 13^6 = 4'826'809$ dwustanowych maszyn Turinga używających trzech symboli (w tym symbolu pustego).

Najmniejsza Uniwersalna Maszyna Turinga



Hipoteza Churcha-Turinga

- W 1936 roku Alonzo Church i Alan Turing zaproponowali niezależnie od siebie różne modele obliczeń: Church wymyslił rachunek lambda a Turing abstrakcyjną maszynę nazwaną później na jego cześć maszyną Turinga.
- Chociaż oba formalizmy bardzo się różnią Turing udowodnił wkrótce, że są one równoważne.
- W 1943 roku Stephen Kleene sformułował następujący wniosek zwany hipotezą (również tezą) Churcha-Turinga: Każdy problem, który może być intuicyjnie uznany za obliczalny, jest rozwiązywalny przez maszynę Turinga.
- Sformułowanie "intuicyjnie uznany za obliczalny" uniemożliwia przeprowadzenie matematycznego dowodu tej hipotezy.

Rozszerzenia maszyn Turinga

Poniższe rozszerzone modele maszyn Turinga mają taką samą moc obliczeniową jak oryginalna maszyna Turinga:

- Maszyny Turinga z wieloma niezależnymi głowicami.
- Maszyny Turinga z wieloma taśmami.
- Maszyny Turinga z taśmą dwuwymiarową.
- Niedeterministyczne maszyny Turinga.
- Probabilistyczne maszyny Turinga.

Równoważność powyższych modeli stanowi argument przemawiający za prawdziwością hipotezy Churcha-Turinga

Maszyny Turinga z ograniczeniami

Poniższe ograniczone modele maszyn Turinga mają taką samą moc obliczeniową jak oryginalna maszyna Turinga:

- Maszyny Turinga z jednostronnie ograniczoną taśmą.
- Maszyny Turinga nad alfabetem binarnym.
- Dwustanowe maszyny Turinga.
- Maszyny Turinga, które nigdy nie nadpisują zapisanych symboli.
- Maszyny Turinga, dla których poprzedni stan może być zawsze jednoznacznie wyznaczony przez stan bieżący oraz przez zawartość taśmy.

Równoważność powyższych modeli stanowi kolejny argument przemawiający za prawdziwością hipotezy Churcha-Turinga

Inne modele obliczeń równoważne z TM

- Systemy formalne Posta (Emil Post 1920) – reguły zamiany słów zaprojektowane do dowodzenia twierdzeń ze zbioru aksjomatów.
- Funkcje ogólnie rekurencyjne (Kurt Gödel 1934).
- Funkcje częściowo rekurencyjne (Alonzo Church 1932, Stephen Kleene 1935).
- Algorytmy Markova (1960) – reguły zamiany słów w ustalonej kolejności.
- Gramatyki nieograniczone (Noam Chomsky 1950)
- Logika klauzul Horna (Horn 1951) – system dowodzenia twierdzeń stanowiący podstawę dla języka programowania Prolog.
- Języki programowania: C, C++, Java, Python, Ruby, Perl, Lisp, . . .