Maszyny Turinga, teoria złożoności i kryptografia

Tomasz Koberda[1]

[1]Wydział Matematyki
University of Virginia, Charlottesville, VA, USA

Wykład popularny w Warszawie, 24 maj 2019

Czym jest teoria obliczeń i teoria złożoności: I

- Jakie funkcje można obliczyć przez procesy automatyczne?
- Jakie są rozsądne modele obliczenia?
- Dany model obliczenia oraz funkcję obliczalną, ile zasobów (to znaczy czasu i miejsca) wymaga jej obliczenie?
- Dane dwie różne funkcje obliczalne, w jaki sposób można porównać stosunkową trudność ich obliczenia?

Czym jest teoria obliczeń i teoria złożoności: II

Przykład: kolorowanie w teorii grafów

- Graf się składa z wierzchołków i z krawędzi między nimi.
- Kolorowanie grafu polega na przepisywaniu wierzchołkom koloru w sposób poprawny, to znaczy żeby wierzchołki styczne jednej krawędzi miały różne kolory.
- Liczba chromatyczna skończonego grafu Γ, to najmniejsza ilość kolorów potrzebna do poprawnego kolorowania Γ.
- Czy liczba chromatyczna jest obliczalna? Tak!

Czym jest teoria obliczeń i teoria złożoności: III

- Prymitywny algorytm do obliczenia liczby chromatycznej jest mało sprawny. Pomiar zasobów wymaganych aby sprawdzić poprawność każdego z tych zabarwień wynosi funkcję co najmniej potęgową w V.
- Sprawne algorytmy istnieją w niektórych klasach grafów. Na przykład, zdecydować czy wystarczą dwa kolory (tzn. czy dany graf jest grafem dwudzielnym) jest obliczalne liniowymi zasobami.
- Dla ogólnych grafów, obliczenie liczby chromatycznej należy do problemów "NP-hard", i teoretyczne cechy ich złożoności są tematem problemu "P vs. NP".

Maszyny Turinga: I

Maszyny Turinga są powszechnym teoretycznym modelem obliczenia.

- Maszyna się posuwa po nieskończonej taśmie na której jest dany wkład, wyrażony liczbą dwójkową.
- Maszyna ma skończoną ilość stanów wewnętrznych, oznaczane liczbami dwójkowymi, i zaczyna w stanie 0.
- Maszyna odczytuje jedynkę lub zero na taśmie. Przy odczycie, zmienia ona stan wewnętrzny, może zamienić zero na jedynkę lub odwrotnie, i może się przysunąć w lewo lub w prawo.
- Maszyna może zatrzymać się w stanie końcowym, lub może działać w nieskończoność.
- Przekształcony ciąg jedynek i zer po zachamowaniu jest danym wyjściowym maszyny na dany wkład.

Maszyny Turinga: II

Funkcja jest obliczalna jeśli istnieje maszyna Turinga co ją oblicza.

- Wykazywanie funkcję nieobliczalną jest nieoczywiste, ale dowód jej istnienia jest prosty.
- Liczność wszystkich funkcji obliczalnych jest przeliczalna, ponieważ tylko istnieje skończona liczność maszyn Turinga z daną skończoną licznością stanów. Liczność funkcji $f : \mathbb{N} \to \mathbb{N}$ jest nieprzeliczalna, i na skutek tego, "prawie że wszystkie" funkcje $f : \mathbb{N} \to \mathbb{N}$ są nieobliczalne.

Teoria złożoności, między innymi według Kolmogorowa

- Dane matematyczne, aby mogła je przerobić maszyna Turinga, muszą być zakodowane liczbą dwójkową.
- Różne maszyny można stosować do tego samego obliczenia, o różnych sprawnościach.
- Jaki jest najkrótszy algorytm co jest w stanie wytworzyć dany ciąg? (Klasyczna złożoność Komogorowa)
- Jaki jest najkrótszy (najprostszy, najszybszy) algorytm co przekształci dany ciąg na dobrany do niego drugi ciąg? To znaczy, jak najszybciej można obliczyć daną funckcję?

Na czym polegają współczesne protokoły kryptograficzne?

- Protokoły kryptograficzne służą do potajemnego przekazywania wiadomości.
- Dwóch rozmówców A i B przekazują sobie wiadomości kanałem który podsłuchuje podsłuchujący E.
- A i B się umawiają z gory jaki ma być zastosowany klucz do odszyfrowania wiadomości.
- Klucz jest często rozwiązaniem zagadnienia z teorii obliczeń, co jest "łatwy" do sprawdzenia ale "trudny" do obliczenia.
- A i B szybko odszyfrowują wiadomość, lecz E wymaga dużych zasobów czasowych aby podobnie odszyfrować przekazane dane.

Przykład: protokół RSA: I

Protokół RSA (Rivest–Shamir–Adleman), to jeden z pierwszych i najpowszechniejszych protokołów kryptograficznych. Polega on na obliczeniach w arytmetyce modularnej.

- Następujące zadanie jest stosunkowo łatwe: znaleść trzy liczby całkowite e, d, n ($> 2^{2000}$) takie że dla każdej liczby całkowitej $0 \leqslant m < n$, mamy równanie modularne

$$(m^e)^d \equiv m \pmod{n}.$$

- Następujące zadanie jest stosunkowo trudne: jeśli mamy dane e oraz n jak w poprzednim równaniu, znaleść d.

Przykład: protokół RSA: II

- W praktycznych zastosowaniach, $n = pq$, gdzie p i q są liczbami pierwszymi wybranymi losowo. Ich iloczyn stanowi część kluczu publicznego, ale p i q są trzymane w tajemnicy.
- Nazwiemy $\lambda(n)$ najmniejszą wspólną wielokrotnością $p-1$ i $q-1$, i wartość $\lambda(n)$ też jest trzymana w tajemnicy.
- Wybierzemy e, dowolną liczbę całkowitą aby e i $\lambda(n)$ były względnie pierwsze. Liczba e też stanowi część kluczu publicznego.
- Potęgę d wybierzemy aby była rozwiązaniem równania

$$d \cdot e \equiv 1 \pmod{\lambda(n)},$$

i ona stanowi klucz prywatny.

Kryptografia na podstawie grup: I

Protokoły kryptograficzne n.p. RSA polegają na arytmetyce liczb całkowitych i na obliczeniowych trudnościach co się tam znajdują. Teoria grup, szczególnie tzw. grup nieabelowych, jest bogatszym źródłem "arytmetyki" w kontekście nieprzemiennym.

Kryptografia na podstawie grup: II

Przykład grupy i obliczenia arytmetycznego:

- $S = \{s, t\}$, $R = \{st^2s^{-1} = t^3\}$. Piszemy: $G = \langle s, t \mid st^2s^{-1} = t^3 \rangle$.
- Czy słowo $w = t^{-3}s^{-1}t^{-3}st^5$ jest trywialne? Tak! Dowód?

Kryptografia na podstawie grup: III

- Jednym z podstawowych problemów teorii grup jest tak zwane pierwsze zagadnienie Dehna: dany skończony alfabet S i skończony zbior R słów trywialnych, czy istnieje algorytm (maszyna Turinga) co jest zdolny zdecydować czy słowo $w \in G = \langle S \mid R \rangle$ jest równe elementowi neutralnemu? Nie! Możliwe jest zakodowanie funkcji nieobliczalnej do zbioru R.
- Kategoria grup jest bardzo bogata, i znajduje się duża rozmaitość zagadnień "arytmetycznych" które nie wkraczają w sferę nieobliczalności lecz wykazują ciekawe zachowanie względem złożoności, na skutek czego nadają się do zastosowań kryptograficznych.

Kierunki kwantowe

Komputery kwantowe znajdują spore zastosowanie w kryptografii, do szyfrowania i również do łamania szyfrów.

- Komputery kwantowe mogą przyspieszyć obliczenia klasycznych maszyn Turinga, więc sformułowanie teorii złożoności kwantowej się różni w znaczny sposób od klasycznej (nie-kwantowej) teorii. (Przykład: algorytm faktoryzacji Shora zagraża protokołowi RSA).
- Komputery kwantowe można modelować wiernie klasycznymi maszynami Turinga, więc kategorie obliczalności i nieobliczalności są niezmienione wprowadzeniem metod kwantowych.
- W jaki sposób można badać grupy nieskończone komputerami kwantowymi?

Kodowanie Gödela i uniwersalna maszyna Turinga

Maszyny Turinga dają sposób zakodowania logiki w jednostce automatycznej.

- Kodowanie Gödela przekształca wyrażenia w języku logiki w liczbę całkowitą. Każdy symbol w alfabecie dozwolonych działań logicznych ma do siebie przypisaną liczbę całkowitą. Kolejność działań w wyrażeniu jest zakodowana za pomocą liczb pierwszych.
- Uniwersalna maszyna Turinga jest algorytmem który jest zdolny odtworzyć wszelki algorytm przez rozszyfrowanie odwrotem kodowania Gödela.

Aksjomatyzacja teorii mnogości

Teoria mnogości jest zaksjomatyzowana ogólnie przyjętymi aksjomatami Zermela–Fraenkla.

- Aksjomaty Zermela–Fraenkla stanowią niesprzeczne podparcie do badania zbiorów.
- Aksjomaty Zermela–Fraenkla są twórcze, w tym sensie że postulują istnienie zbiorów niepustych, oraz zbiorów nieskończonych, przez proces induktywny.
- Istnieją zagadnienia dotyczące zbiorów które są logicznie niezależne od aksjomatów Zermela–Fraenkla. Jeden z bardziej znanych przykładów tego jest hipoteza continuum.

Teoria mnogości i maszyny Turinga

- W latach sześćdziesiątych, Rado skonstruował funkcję tak zwaną Busy Beaver $BB : \mathbb{N} \to \mathbb{N}$ która rośnie szybciej niż dowolna funkcja obliczalna.
- $BB(n)$ jest, w pewnym sensie, największą liczbą całkowitą obliczalną maszyną Turinga składającej się z nie więcej niż n stanów.
- Funkcja $BB(n)$ jest otrzymana w sposób deterministyczny, lecz okrężny.
- Wartości $BB(n)$ dla stosunkowo niewielkich wkładów n (< 8000) są niezależne od aksjomatów Zermela–Fraenkla.
- Zachowanie funkcji $BB(n)$ sugeruje paradoksalne konsekwencje w filozofii matematyki.

Koniec

Dziękuję!