EITC/FC/CCT

Złożoność obliczeniowa jako podstawa bezpieczeństwa informacji

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie i model obliczeniowy oparty o maszynę Turinga
    - Model obliczeń
    - Maszyna Turinga
        - Definicja formalna
        - Działanie
        - Reprezentacja
    - Język maszyny. Języki rekurencyjne i rekurencyjnie przeliczalne
    - Zapis programu i stanu maszyny
    - Zasoby potrzebne do obliczenia maszyny
    - Wielotaśmowa maszyna Turinga
    - Niedeterministyczna maszyna Turinga
- Inne modele dla złożoności
    - Maszyna RAM
        - Zestaw instrukcji
        - Działanie maszyny RAM
        - Rozpoznawanie języków
        - Złożoność obliczeniowa w modelu RAM
        - Porównanie czasu działania maszyny Turinga i maszyny RAM
        - Symulowanie maszyny RAM na wielotaśmowej maszynie Turinga
        - Porównanie złożoności pamięciowej w modelach obliczeniowych
    - Obwody logiczne
- Klasy złożoności obliczeniowej
    - Klasy złożoności czasowej i pamięciowej
    - Twierdzenia o liniowym przyspieszaniu i kompresji pamięci
    - Relacje między klasami, twierdzenie Savitcha
    - Dopełnienia klas
    - Twierdzenia o hierarchii czasowej i pamięciowej
- Redukcje, zupełność oraz problemy NP-zupełne
    - Redukcje wielomianowe, logarytmiczne i transformacje
        - Redukcje wielomianowe
        - Redukcje logarytmiczne
        - Transformacja wielomianowa w sensie Turinga
    - Zupełność
    - Klasa NP i NP-zupełność
        - Problem SAT
        - Charakteryzacja klasy NP w języku logiki
        - Egzystencjalne zdania drugiego rzędu a złożoność
        - Twierdzenie Fagina
    - Problem SAT
        - 3SAT
        - MAXSAT
    - NP-zupełne problemy grafowe
        - Pokrycie wierzchołkowe
        - Klika, zbiór niezależny
    - Problemy na zbiorach i liczbach
        - Trójdzielne skojarzenie i pokrycie zbiorami
        - Suma podzbioru i inne problemy liczbowe
- Algorytmy i schematy aproksymacji

- Problem optymalizacyjny
    - Problemy optymalizacyjne a problemy decyzyjne
    - Rozwiązania aproksymacyjne
  - Pokrycie wierzchołkowe NODE COVER
    - Algorytm zachłanny
    - Algorytm skojarzeniowy
  - Problem maksymalnego przekroju MAX CUT
  - Problem komiwojażera TSP
    - Wersja metryczna
  - Pakowanie BIN PACKING
    - 2-aproksymacja
  - Problem plecakowy KNAPSACK
  - Schematy aproksymacji
  - Schemat aproksymacji dla problemu KNAPSACK
  - Asymptotyczny PTAS dla BIN PACKING
  - L-redukcje
- Algorytmy probabilistyczne
  - Probabilistyczne klasy złożoności
    - Klasa ZPP
    - Klasa PP
    - KLASA BPP
  - Rozpoznawanie liczb pierwszych
    - Test Millera-Rabina
  - Generowanie bitów losowych
- Obliczenia równoległe
  - Modele obliczeń równoległych
    - PRAM
    - Obwody logiczne
  - Klasy złożoności
    - Model obwodów logicznych
    - Klasy w modelu PRAM
  - P-zupełność
  - Równoległość i randomizacja
- Problemy funkcyjne i złożoność zliczania
  - Problemy funkcyjne
    - Klasy FP i FNP
    - Klasa TFNP
  - Złożoność zliczania
    - Klasa 'hasz P' i twierdzenie Valianta
    - Klasa 'parzystość P'
- Pamięć logarytmiczna, hierarchia wielomianowa, pamięć wielomianowa i złożoność wykładnicza
  - Klasy L, NL i coNL
  - Twierdzenie Immermana-Szelepcsényi'ego
  - Klasy coNP i DP
  - Maszyny alternujące
  - Hierarchia wielomianowa
  - Klasa PSPACE
  - Problemy PSPACE-zupełne
    - Optymalizacja periodyczna
  - Złożoność wykładnicza
    - Problemy zwięzłe
    - Wyrażenia regularne
- Kryptografia a złożoność
  - Funkcje jednokierunkowe
  - Systemy dowodów interaktywnych