Podstawy systemów dyskretnych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Podstawy systemów dyskretnych
Kod przedmiotu	11.9-WE-INFP-PodstSystDyskr
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Informatyka
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. inżyniera
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie

Semestr	2
Liczba punktów ECTS do zdobycia	5
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• prof. dr hab. Roman Gielerak

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	30	2	18	1,2	Egzamin
Laboratorium	15	1	9	0,6	Zaliczenie na ocenę
Ćwiczenia	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

- zapoznać studentów z podstawowymi metodami i technikami matematyki dyskretnej stosowanych w rożnych obszarach informatyki takich jak np. analiza algorytmów ,kryptografia i analiza danych.

- wyjaśnienie na bazie algorytmiki teorio- liczbowej podstaw złożoności obliczeniowej współczesnych algorytmów szyfrowania

- nauczenie stosowania wymienionych metod matematycznych do rozwiązywania zadań praktycznych pojawiających sie w praktyce

-obsługa środowiska skryptowego Maple

Wymagania wstępne

Analiza matematyczna, Algebra liniowa z geometrią analityczną, Logika dla informatyków

Zakres tematyczny

Wstęp: elementarne własności funkcji i ciągów (terminologia i notacja). Algebra zbiorów , algebra Boola.

Relacje: Relacje jako zbiory, relacje vs. grafy i vs. macierze. Podziały na klasy abstrakcji. Relacje porządkujące.

Procedury indukcyjne i rekurencyjne : Zachowania asymptotyczne: notacje ?, ?, o(-), O(-). Indukcja matematyczna i jej zastosowania. Wzór dwumienny Newtona. Procedury indukcyjne. Definicje i procedury rekurencyjne. Równania rekurencyjne. Liniowe równania rekurencyjne i ich rozwiązywanie. Metoda wielomianu charakterystycznego i metoda szeregów potęgowych. Funkcjonał generujący. Uniwersalne rekurencje i ich zastosowania do analizy złożoności obliczeniowych algorytmów rekurencyjnych. Algorytm Euklidesa i analiza jego złożoności obliczeniowej. Liczby Fibonacciego. Algorytmy rekurencyjne i indukcyjne.

Zagadnienia kombinatoryczne. Elementarne procedury zliczania. Podziały. Algorytmy teoriomnogościowe. Zasada szufladkowa Dirichleta. Permutacje. Kombinacje. Wariacje. Funkcje generujące. Algorytmy kombinatoryczne i ich złożoność obliczeniowa. Zastosowania do elementarnej teorii prawdopodobieństwa.

Zagadnienia teorii grafów. Grafy i grafy skierowane. Zastosowania rachunku macierzy do analizy grafów. Algorytmy na grafach skierowanych. Zagadnienia i algorytmy na grafach: przeszukiwania, sortowania, szukanie drzew rozpinających, szukanie optymalnych ścieżek. Optymalne przepływy na grafach. Problem komiwojażera.

Zagadnienia teorioliczbowe. Relacje podzielności. Arytmetyka modularna. Liniowe równania modularne. Chińskie twierdzenie o resztach. Rząd elementu: logarytm dyskretny. Problem faktoryzacji: twierdzenie Eulera i twierdzenie (małe) Fermata. Protokół kryptograficzny RSA. Testy pseudopierwszości. Test RabinaMillera.

Elementy logiki. Kwantyfikatory. Elementarny rachunek predykatów.

Zbiory nieskończone. Sieci boolowskie. Tablice Karnaugha.

Uzupełnienia. Języki formalne. Klasyczna teoria złożoności obliczeniowej. Problemy NP. i NP-zupełne.

Metody kształcenia

wykład: wykład konwencjonalny

ćwiczenia: konsultacje, ćwiczenia rachunkowe

laboratorium: implementacje algorytmow do środowiska Maple

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Znajomość podstawowych metod i technik matematyki dyskretnej w zadaniach informatyki oraz praktyczna obsługa środowiska obliczeniowego Maple	• K_W01 • K_U05 • K_U09 • K_K01	• bieżąca kontrola na zajęciach • egzamin - ustny, opisowy, testowy i inne • kolokwium	• Wykład • Ćwiczenia
Umiejętność analizowania relacji za pomocą metod teorii grafów i rachunku macierzowego	• K_W01 • K_U05 • K_U09	• bieżąca kontrola na zajęciach • egzamin - ustny, opisowy, testowy i inne • kolokwium	• Wykład • Ćwiczenia
Znajomość algorytmów teorioliczbowych stosowanych w kryptografii asymetrycznej	• K_W01 • K_W08 • K_U05	• bieżąca kontrola na zajęciach • egzamin - ustny, opisowy, testowy i inne • kolokwium	• Wykład • Ćwiczenia
Umiejętność szacowania złożoności obliczeniowych procedur rekurencyjnych oraz stosowania zasad indukcji matematycznej	• K_W01 • K_U05 • K_U09	• bieżąca kontrola na zajęciach • egzamin - ustny, opisowy, testowy i inne • kolokwium	• Wykład • Ćwiczenia
Znajomość elementarnych algorytmów kombinatorycznych	• K_W01 • K_U05 • K_U09	• bieżąca kontrola na zajęciach • egzamin - ustny, opisowy, testowy i inne • kolokwium	• Wykład • Ćwiczenia

Warunki zaliczenia

Wykład - warunkiem zaliczenia jest rozwiązanie ponad 60% zadań egzaminacyjnych

Ćwiczenia - warunkiem zaliczenia jest uzyskanie oceny pozytywnej z ponad 66% realizowanych kolokwiów

Laboratorium-warunkiem zaliczenia jest uzyskanie oceny pozytywnej z ponad 66% realizowanych kolokwiów

Ocena końcowa: średnia arytmetyczna ocen z egzaminu i zaliczenia ćwiczeń i laboratorium

Literatura podstawowa

1. Ross, K.A., Wright, Ch.R.B., Matematyka Dyskretna, Warszawa, PWN, 2006.
2. Jabłoński S.W., Wstęp do matematyki dyskretnej, Warszawa, PWN, 1991.
3. Cormen, T.H., Leiserson Ch.E., Rivest R.L., Wprowadzenie do algorytmów, Warszawa, WNT, 1997.
4. Ben-Ari, M., Logika matematyczna, Warszawa, WNT, 2005.
5. Deo, N., Teoria grafów i jej zastosowania w technice i informatyce, Warszawa, PWN, 1980.

Literatura uzupełniająca

1. Reingold E.M., Nievergelt J., Deo N.: Algorytmy kombinatoryczne, PWN, Warszawa, 1985.
2. Flachmeyer J.: Kombinatoryka, PWN, Warszawa, 1987

Uwagi

Zmodyfikowane przez prof. dr hab. Roman Gielerak (ostatnia modyfikacja: 25-04-2018 13:25)