

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: M

Stopień studiów: I

Specjalności: Modelowanie matematyczne

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Kodowanie algebraiczne
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	
KOD PRZEDMIOTU	WFMiI M oIS C1 14/15
KATEGORIA PRZEDMIOTU	Przedmioty kierunkowe
LICZBA PUNKTÓW ECTS	4.00
SEMESTRY	5

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
5	30	30	0	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Nacyzyć studentów podstawowych pojęć i metod niezbędnych we współczesnym kodowaniu algebraicznym

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Algebra liniowa z geometrią analityczną, podstawy algebry abstrakcyjnej, elementy teorii liczb oraz logika i matematyka dyskretna

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student zna podstawowe pojęcia teorii ciał skończonych i zagadnienia o ciągach pseudolosowych

EK2 Wiedza Student zna podstawy teorii Shannona (pojęcia oraz twierdzenia), kodowania liniowego i cyklicznego

EK3 Umiejętności Student wie i demonstruje jak zrealizować działania w ciałach skończonych, może budować ich tabelki Cayleya, kodować i dekodować informację za pomocą różnych kodów liniowych i cyklicznych

EK4 Kompetencje społeczne Student nie tylko wie i demonstruje jak zrealizować działania w ciałach skończonych, może budować ich tabelki Cayleya, kodować i dekodować informację za pomocą różnych kodów liniowych i cyklicznych, lecz również potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych

6 TREŚCI PROGRAMOWE

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Wstęp: elementy transmisji danych, charakterystyka kodów, typy kodów, struktura kodu blokowego, zdolność detekcyjna, zdolność korekcyjna	2
W2	Teoria ciał skończonych: rozszerzenie ciał, wielomian minimalny elementu algebraicznego, ciała skończone, automorfizmy ciał skończonych. podciała ciała F_q , wielomiany nierozkładalne i pierwotne nad ciałem F_q , cykliczność grupy multiplikatywnej ciała skończonego i elementy pierwotne	6
W3	Realizacja działań w ciałach skończonych: logarytmy Żecha, układy realizujące działania arytmetyczne w ciałach skończonych i ich programowa realizacja	2
W4	Teoria Shannona o kodowaniu: tajność doskonała, entropija, jej własności, twierdzenie Shannona o kodowaniu	2
W5	Kody liniowe: długość i waga Hamminga, odległość minimalna kodu, macierzowy opis kodu, tablica standardowa, kodowanie i dekodowanie informacji, operacje nad kodami	4
W6	Ciągi pseudolosowe: okresowe ciągi nad ciałami skończonymi, wielomiany pierwotne nad ciałami skończonymi, konstruowanie ciał skończonych	4
W7	Kody cykliczne: charakterystyka kodów cyklicznych, wielomiany generujące i sprawdzające kod cykliczny, kodowanie i dekodowanie kodów cyklicznych, macierzowy opis kodów cyklicznych	4
W8	Kody cykliczne binarne: kody hamminga, kody maksymalnej długości, kody BCH, ich kodowanie i dekodowanie	4

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W9	Inne kody: kody Reeda-Solomona, kody goppaego i inne	2

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Badanie rozszerzenia ciał, wielomianów minimalnych elementów algebraicznych, ciał skończonych, automorfizmy ciał skończonych. podciała ciała F_q , wielomiany nierozkładalne i pierwotne nad ciałem F_q , cykliczność grupy multiplikatywnej ciała skończonego i elementy pierwotne	4
C2	Obliczenia w ciałach skończonych: logarytmy żecha, układy realizujące działania arytmetyczne w ciałach skończonych i ich programowa realizacja	2
C3	Teoria Shannona o kodowaniu: tajność doskonała, entropija, jej własności, twierdzenie Shannona o kodowaniu, entropia	4
C4	Obliczenia na kodach liniowych: długość i waga Hamminga, odległość minimalna kodu, macierzowy opis kodu, tablica standardowa, kodowanie i dekodowanie informacji, operacje nad kodami	8
C5	Konstruowanie ciągów pseudolosowych: okresowe ciągi nad ciałami skończonymi, wielomiany pierwotne nad ciałami skończonymi, konstruowanie ciał skończonych	4
C6	Obliczenia na kodach cyklicznych: charakterystyka kodów cyklicznych, wielomiany generujące i sprawdzające kod cykliczny, kodowanie i dekodowanie kodów cyklicznych, macierzowy opis kodów cyklicznych	4
C7	Kody cykliczne binarne, obliczenia: kody hamminga, kody maksymalnej długości, kody BCH, ich kodowanie i dekodowanie	2
C8	Badania innych kodów: kody Reeda-Solomona, kody goppaego i inne	2

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Dyskusja

N3 Konsultacje

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	0
Konsultacje przedmiotowe	0
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	60
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	60
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	4.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Kolokwium

OCENA PODSUMOWUJĄCA

P1 Zaliczenie pisemne

P2 Zaliczenie ustne

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Do zaliczenia przystępują studenci, którzy zaliczyli algebrę liniową z geometrią analityczną oraz algebrę abstrakcyjną

W2 Ocena końcowa jest średnią ocen P1 i P2

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie zna podstawowych pojęć o kodowaniu, ciałach skończonych i ciągach pseudolosowych
NA OCENĘ 3.0	Student zna podstawowe pojęcia o kodowaniu, ciałach skończonych i ciągach pseudolosowych, ilustruje ich przykładami

NA OCENĘ 3.5	Student zna podstawowe pojęcia i podstawowe zagadnienia o kodowaniu, ciałach skończonych i ciągach pseudolosowych, ilustruje ich przykładami
NA OCENĘ 4.0	Student zna podstawowe pojęcia o kodowaniu, może udowodnić podstawowe zagadnienia o ciałach skończonych i ciągach pseudolosowych, ilustruje ich przykładami
NA OCENĘ 4.5	Student zna podstawowe pojęcia o kodowaniu, ciałach skończonych i ciągach pseudolosowych, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych zadań teoretycznego i praktycznego charakteru
NA OCENĘ 5.0	Student zna podstawowe pojęcia o kodowaniu, ciałach skończonych i ciągach pseudolosowych, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia o ciałach skończonych i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie zna podstawowych pojęć o kodowaniu liniowym i cyklicznym
NA OCENĘ 3.0	Student zna podstawowe pojęcia o kodowaniu liniowym i cyklicznym oraz ilustruje ich przykładami
NA OCENĘ 3.5	Student zna podstawowe pojęcia i podstawowe zagadnienia o kodowaniu liniowym i cyklicznym oraz ilustruje ich przykładami
NA OCENĘ 4.0	Student zna podstawowe pojęcia i podstawowe zagadnienia o kodowaniu liniowym i cyklicznym, może udowodnić podstawowe zagadnienia, zilustrować przykładami oraz rozwiązywaniem zadań elementarnych
NA OCENĘ 4.5	Student zna podstawowe pojęcia i podstawowe zagadnienia o kodowaniu liniowym i cyklicznym, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych zadań oraz ilustruje ich przykładami
NA OCENĘ 5.0	Student zna podstawowe pojęcia o kodowaniu liniowym i cyklicznym, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie zna podstawowych pojęć oraz nie może rozwiązać zadań elementarnych
NA OCENĘ 3.0	Student zna podstawowe pojęcia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować podstawowe pojęcia przykładami
NA OCENĘ 3.5	Student zna podstawowe pojęcia i zagadnienia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować ich przykładami
NA OCENĘ 4.0	Student zna podstawowe pojęcia i zagadnienia z dowodami, umie rozwiązać podstawowe zadania praktycznego i teoretycznego charakteru i zilustrować ich przykładami

NA OCENĘ 4.5	Student zna podstawowe pojęcia, ich związki oraz zagadnienia z dowodami, umie rozwiązać zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami
NA OCENĘ 5.0	Student zna podstawowe pojęcia i podstawowe zagadnienia, ich związki oraz zagadnienia z dowodami, umie rozwiązać standardowe i niestandardowe zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami i stosować na praktyce
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie zna ograniczenia własnej wiedzy, nie potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu
NA OCENĘ 3.0	Student zna ograniczenia własnej wiedzy, nie potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu
NA OCENĘ 3.5	Student zna podstawowe pojęcia i podstawowe zagadnienia i może ich zilustrować
NA OCENĘ 4.0	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować i udowodnić, rozumie konieczność systematycznej pracy
NA OCENĘ 4.5	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować, udowodnić i rozwiązać podstawowe zadania, rozumie konieczność systematycznej pracy
NA OCENĘ 5.0	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, może ich zilustrować, udowodnić i rozwiązać podstawowe i niestandardowe zadania, rozumie konieczność systematycznej pracy, potrafi samodzielnie wyszukiwać informacje w literaturze, także w językach obcych

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	K_W01, K_W02, K_W03, K_W04, K_W05	Cel 1	W1 W2 W3 W4	N1 N2 N3	F1 P1 P2

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK2	K_W01, K_W02, K_W03, K_W04, K_W05	Cel 1	W5 W6 W7 W8 W9	N1 N2 N3	F1 P1 P2
EK3	K_U01, K_U02, K_U05, K_U36	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2 N3	F1 P1 P2
EK4	K_K01, K_K02, K_K05, K_K07	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2 N3	F1 P1 P2

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | W. Mochnacki — *Kody korekcyjne i kryptografia*, Wrocław, 1997, PW
- [2] | Z. Szwaja — *Realizacja binarnych kodów Bose-Chaudhuri-Hocqenghema*, Poznań, 1968, PP
- [3] | A. Politowska — *Algebraiczne aspekty teorii kodów*, Warszawa, 2008, PWar
- [4] | J. Drózd — *Podstawy kodowania nadmiarowego*, Warszawa, 1968, PWars
- [5] | C. Kościelny — *Programowa realizacja działań w ciałach skończonych do zastosowań w technice i kryptologii*, Wrocław, 1983, PW

LITERATURA UZUPEŁNIAJĄCA

- [1] | R. Lidl, H. Niederreiter — *Finite fields*, London, 1983, Addison-Wesley
- [2] | E.R. Berlekamp — *Algebraic coding theory*, New York, 1968, McGraw-Hill
- [3] | Shu Lin — *An introduction to Error-Correcting Codes*, London, 1970, Prentice-Hall Inc.

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. Orest Artemowicz (kontakt: artemo@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

- 1 Prof. dh hab. Orest Artemowicz (kontakt: artemo@usk.pk.edu.pl)



13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....