

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka Stosowana

Profil: Praktyczny

Forma studiów: stacjonarne

Kod kierunku: MS

Stopień studiów: I

Specjalności: Matematyka w finansach i ekonomii

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Kodowanie algebraiczne
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Algebraic coding
KOD PRZEDMIOTU	WiT MS pIS D10 22/23
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	5.00
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 1.Nauczenie studentów podstawowych metod kodowania algebraicznego, intensywnie stosowanych we współczesnej informatyce, telekomunikacji itp.

Cel 2 2.Uzupełnienie i pogłębienie wiedzy studentów w zakresie algebry (zwłaszcza teorii ciał).

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 zaliczenie przedmiotów „Algebra liniowa z geometrią analityczną”, „Algebra z teorią liczb oraz”, „Rachunek prawdopodobieństwa”.

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza 1.Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałami (K_W04).

EK2 Wiedza 2.Student zna i rozumie podstawowe pojęcia i twierdzenia teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe przykłady kodów (K_W01, K_W05, K_W26).

EK3 Umiejętności 3.Student potrafi rozwiązywać zadania i problemy o charakterze praktycznym dotyczące typowych kodów i ich własności (K_U08, K_U09).

EK4 Kompetencje społeczne 4.Student jest przygotowany do poszerzania swojej wiedzy z algebraicznej teorii kodowania i do dzielenia się tą wiedzą z niematematykami (K_U29, K_U35, K_K01).

6 TREŚCI PROGRAMOWE

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Arytmetyka liczb całkowitych: Twierdzenie o dzieleniu z resztą, pierścień klas reszt modulo n . Ciało proste F_p .	1
W2	Ciała skończone: Istnienie i jedyność. Grupa multiplikatywna ciała skończonego, jej cykliczność. Elementy prymitywne. Automorfizmy Frobeniusa.	2
W3	Wielomiany nad ciałami skończonymi: Pierścień $F_p[X]$. Wielomiany nieprzywiedlne nad ciałem F_p . Pierścień ilorazowy $F_p[X]/(f)$, gdzie f to wielomian nieprzywiedlny nad F_p . Wielomiany prymitywne. Postać macierzowa ciała skończonego. Liniowe ciągi rekurencyjne. Postać wektorowa ciała skończonego. Wielomiany minimalne, warstwy cyklotomiczne, faktoryzacja wielomianu $X^n - 1$ nad ciałem skończonym.	4
W4	Kody i entropia: Alfabet, słowa i kody. Proste przykłady kodów (ISBN, EAN-13, Morse itp.). Kanał transmisji danych. Entropia źródła. Twierdzenie Krafta-McMillana. Podstawowe twierdzenie Shannona o bezsumowym kodowaniu dyskretnym. Entropia języka.	2
W5	Elementarne własności informacji: Entropia warunkowa. Informacja wzajemna. Przepustowość kanału. Drugie twierdzenie Shannona.	2
W6	Kody liniowe: Metryka Hamminga. Wykrywanie i korygowanie błędów. Dekodowanie z maksymalną wiarygodnością. Dekodowanie do najbliższego słowa kodowego. Kody liniowe, ich równoważność i kody dualne. Macierzowy opis kodów liniowych. Kodowanie i dekodowanie za pomocą kodów liniowych.	4
W7	Ograniczenia na pojemność kodów: Kody doskonałe, kody optymalne.	2

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W8	Kody cykliczne: Własności elementarne. Wielomianowy i macierzowy opis kodów cyklicznych. Kodowanie i dekodowanie. Kody reszt kwadratowych.	4
W9	Piękne kody: Binarne i niebinarne kody Hamminga. Kody Golaya. Kod Vasileva.	3
W10	Działania na kodach.	2
W11	Kody BCH: Własności elementarne. Kryterium większościowe (majority logic decoding). Kody Reeda-Solomona. Kody Reeda-Mullera. Kodowanie i dekodowanie.	4

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Arytmetyka liczb całkowitych: Zapisywanie liczb całkowitych w systemie dwójkowym, szesnastkowym i notacji rzymskiej. Sprawdzanie, czy dana liczba jest pierwsza. Sito Eratostenesa. Znajdowanie postaci kanonicznej liczb całkowitych. Wyznaczanie NWD i NWW.	2
C2	Arytmetyka modularna: Obliczanie wartości funkcji Eulera. Znajdowanie elementów odwrotnych w pierścieniach klas reszt. Rozwiązywanie kongruencji liniowych.	1
C3	Wielomiany nad ciałem skończonym: Wielomiany przywiedlne i nieprzywiedlne nad ciałami skończonymi. Wyznaczanie rzędu wielomianu. Sprawdzanie, czy dany wielomian jest prymitywny. Przedstawianie ciał skończonych w postaci macierzowej. Konstruowanie liniowych ciągów rekurencyjnych stowarzyszonych z wielomianami, znajdowanie okresów tych ciągów. Przedstawianie ciał skończonych w postaci wektorowej. Wyznaczanie wielomianu minimalnego elementu ciała skończonego. Warstwy cyklotomiczne. Faktoryzacja wielomianów $X^n - 1$.	4
C4	Kody i entropia: Sprawdzanie poprawności kodowania (dla kodów ISBN, EAN-13, Morse'a itp.). Obliczanie entropii źródła.	2
C5	Elementarne własności informacji: Obliczanie entropii warunkowej oraz informacji wzajemnej. Wyznaczanie przepustowości kanału. Badanie innych własności informacji.	2
C6	Kody liniowe: Wyznaczanie wagi Hamminga słowa i odległości Hamminga między słowami. Badanie zdolności detekcyjnej i zdolności korekcyjnej kodów liniowych. Znajdowanie macierzy generującej i macierzy kontrolnej kodu liniowego. Wyznaczanie kodu dualnego. Kodowanie i dekodowanie za pomocą kodów liniowych.	3

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C7	Kody cykliczne: Opisywanie kodów cyklicznych z danym wielomianem generującym. Znajdowanie wielomianu kontrolnego kodu cyklicznego. Znajdowanie macierzy generującej i macierzy kontrolnej (w postaci standardowej i niestandardowej). Kodowanie i dekodowanie za pomocą kodów cyklicznych w postaci standardowej. Kody reszt kwadratowych.	4
C8	Piękne kody: Kodowanie i dekodowanie za pomocą binarnych i niebinarnych kodów Hamminga. Kodowanie za pomocą kodów Golaya.	2
C9	Działania na kodach: Wykonywanie różnych działań na kodach i opisywanie parametrów otrzymanych w ten sposób nowych kodów.	2
C10	Kody BCH: Kryterium większościowe. Kodowanie i dekodowanie za pomocą kodów BCH, kodów Reeda-Solomona, kodów Reeda-Mullera (pierwszego rzędu) oraz kodów Goppy.	8

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady.

N2 Ćwiczenia tablicowe

N3 Dyskusja.

N4 Konsultacje.

N5 W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo.

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	30
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	55
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	150
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 sprawdziany z bieżącego materiału (na ćwiczeniach) Ocena końcowa z przedmiotu jest średnią arytmetyczną trzech ocen częściowych: z ćwiczeń, z części pisemnej kolokwium zaliczeniowego i z części ustnej kolokwium zaliczeniowego. Wszystkie oceny częściowe muszą być pozytywne.

OCENA PODSUMOWUJĄCA

P1 Ocena końcowa z przedmiotu jest średnią arytmetyczną trzech ocen częściowych: z ćwiczeń, z części pisemnej kolokwium zaliczeniowego i z części ustnej kolokwium zaliczeniowego. Wszystkie oceny częściowe muszą być pozytywne.

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Warunkiem koniecznym i wystarczającym zaliczenia ćwiczeń jest uzyskanie więcej niż połowy maksymalnej sumarycznej liczby punktów ze wszystkich sprawdzianów. Ocena końcowa z przedmiotu jest średnią arytmetyczną trzech ocen częściowych: z ćwiczeń, z części pisemnej kolokwium zaliczeniowego i z części ustnej kolokwium zaliczeniowego. Wszystkie oceny częściowe muszą być pozytywne.

OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Test

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3,0
NA OCENĘ 3.0	Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałem, ilustrując ich przykładami, rozwiązując podstawowe zadania praktyczne
NA OCENĘ 3.5	Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałem, ilustrując ich przykładami, formułując podstawowe zagadnienia, rozwiązując podstawowe zadania praktyczne
NA OCENĘ 4.0	Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałem, ilustrując ich przykładami, formułując zagadnienia i zna ich dowody, rozwiązując podstawowe zadania teoretyczne i praktyczne
NA OCENĘ 4.5	Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałem, ilustrując ich przykładami, formułując zagadnienia i zna ich dowody, rozwiązując standardowe zadania teoretyczne i praktyczne
NA OCENĘ 5.0	Student zna i rozumie podstawy teorii ciał skończonych oraz pierścieni wielomianów i przestrzeni wektorowych nad tymi ciałem, ilustrując ich przykładami, formułując zagadnienia i zna ich dowody, rozwiązując standardowe i niestandardowe zadania teoretyczne i praktyczne
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3,0
NA OCENĘ 3.0	Student zna i rozumie podstawowe pojęcia i twierdzenia teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe przykłady kodów
NA OCENĘ 3.5	Student zna i rozumie podstawowe pojęcia i twierdzenia teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe przykłady kodów i podstawowe algorytmy kodowania i dekodowania
NA OCENĘ 4.0	Student zna i rozumie podstawowe pojęcia i twierdzenia (z dowodami) teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe przykłady kodów i podstawowe algorytmy kodowania i dekodowania
NA OCENĘ 4.5	Student zna i rozumie standardowe pojęcia i twierdzenia (z dowodami) teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe przykłady kodów i standardowe algorytmy kodowania i dekodowania
NA OCENĘ 5.0	Student zna i rozumie standardowe pojęcia i twierdzenia (z dowodami) teorii kodowania oraz jej znaczenie praktyczne. Zna ponadto standardowe i niestandardowe przykłady kodów i algorytmy kodowania i dekodowania
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3,0

NA OCENĘ 3.0	Student potrafi rozwiązywać zadania i problemy o charakterze praktycznym dotyczące typowych kodów i ich własności
NA OCENĘ 3.5	Student potrafi rozwiązywać zadania i problemy, formułować podstawowe zagadnienia o charakterze praktycznym dotyczące typowych kodów i ich własności
NA OCENĘ 4.0	Student potrafi rozwiązywać zadania i problemy, formułować podstawowe zagadnienia (i konstruować ich dowody) o charakterze praktycznym dotyczące typowych kodów i ich własności
NA OCENĘ 4.5	Student potrafi rozwiązywać standardowe zadania i problemy, formułować podstawowe zagadnienia (i konstruować ich dowody) o charakterze praktycznym i teoretycznym dotyczące typowych kodów i ich własności
NA OCENĘ 5.0	Student potrafi rozwiązywać standardowe i niestandardowe zadania i problemy, formułować podstawowe zagadnienia (i konstruować ich dowody) o charakterze praktycznym i teoretycznym dotyczące typowych kodów i ich własności
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3,0
NA OCENĘ 3.0	Student jest przygotowany do poszerzania swojej wiedzy z algebraicznej teorii kodowania i do dzielenia się tą wiedzą praktyczną z niematematykami
NA OCENĘ 3.5	Student jest przygotowany do poszerzania swojej wiedzy praktycznej z algebraicznej teorii kodowania i do dzielenia się tą wiedzą praktyczną, i standardową teoretyczną z niematematykami
NA OCENĘ 4.0	Student jest przygotowany do poszerzania swojej wiedzy podstawowej praktycznej i teoretycznej z algebraicznej teorii kodowania i do dzielenia się tą wiedzą praktyczną, i teoretyczną z niematematykami
NA OCENĘ 4.5	Student jest przygotowany do poszerzania swojej wiedzy standardowej praktycznej i teoretycznej z algebraicznej teorii kodowania i do dzielenia się tą wiedzą praktyczną, i teoretyczną z niematematykami
NA OCENĘ 5.0	Student jest przygotowany do poszerzania swojej wiedzy standardowej i niestandardowej praktycznej i teoretycznej z algebraicznej teorii kodowania i do dzielenia się tą wiedzą praktyczną, i teoretyczną z niematematykami

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	Cel 1 Cel 2	W1 W2 W3 W4 C1 C2 C3 C4	N1 N2 N3 N4	F1 P1
EK2	K_W01	Cel 1 Cel 2	W5 W6 W7 W8 W9 W10 W11 C5 C6 C7 C8 C9 C10	N1 N2 N3 N4	F1 P1
EK3	K_U01	Cel 1 Cel 2	W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10	N1 N2 N3 N4	F1 P1
EK4	K_K01	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10	N1 N2 N3 N4	F1 P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | O.Artemowicz, A. Piękosz — *Algebra*, Kraków, 2010, Wydawnictwo PK
- [2] | A.Pilitowska — *Algebraiczne aspekty kodów*, Warszawa, 2008, Oficyna Wyd. PWars
- [3] | W.Mochnacki — *Kody korekcyjne i kryptografia*, Wrocław, 2000, Oficyna Wyd. PWr
- [4] | C. Bagiński — *Wstęp do teorii grup*, Warszawa, 2001, Skrypt
- [5] | J.Gancarzewicz — *Arytmetyka*, Kraków, 2000, Wyd. UJ
- [6] | M.Bratijczuk, A. Chudziński — *Rachunek prawdopodobieństwa*, Gliwice, 2000, Wyd. PŚ

LITERATURA UZUPEŁNIAJĄCA

- [1] | R.Ash — *Information theory*, NY London Sydney, 1965, Interscience Publ.
- [2] | R.Lidl, H.Niederreiter — *Finite fields*, NY, 1983, Addison-Wesley Publ. Co.
- [3] | R.Hill — *A first course in coding theory*, Oxford, 1986, Clarendon Press
- [4] | R.W.Hamming — *Coding and information theory*, New Jersey, 1980, Prentice-Hall Inc.
- [5] | J.Rutkowska — *Teoria liczb w zadaniach*, Warszawa, 2018, PWN
- [6] | W.Marzantowisz, P.Zarzycki — *Elementy teorii liczb*, Poznań, 1999, Wyd. nauk. UAM

LITERATURA DODATKOWA

- [1] | **J. Wolfowitz** — *Coding theorems and Information Theory*, Berlin Heidelberg New York, 1978, Springer-Verlag
- [2] | **J.H. van Lint** — *Introduction to Coding Theory*, Berlin Heidelberg NY, 1999, Springer-Verlag
- [3] | **S.A. Vanstone, P.C. van Oorschot** — *An introduction to error correcting codes with applications*, Boston Dordrecht London, 1995, Kluwer Acad. Publ.

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH**OSOBA ODPOWIEDZIALNA ZA KARTĘ**

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

OSOBY PROWADZĄCE PRZEDMIOT

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

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....