**Nazwa przedmiotu:**

Kody korekcyjne i transmisja danych

**Koordynator przedmiotu:**

dr hab. inż. Agata Pilitowska, prof. uczelni

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

1 / rok ak. 2023/2024

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. godziny kontaktowe – 65 h; w tym
 a) obecność na wykładach – 30 h
 b) obecność na ćwiczeniach – 30 h
 c) konsultacje – 5 h
2. praca własna studenta – 45 h; w tym
 a) przygotowanie do ćwiczeń i do kolokwiów – 25 h
 b) zapoznanie się z literaturą – 10 h
 c) przygotowanie referatu – 10 h
Razem 95 h, co odpowiada 4 pkt. ECTS

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 30 h
c) konsultacje – 5 h
Razem 65 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

-

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 30h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Przedmioty poprzedzające:
1. Algebra liniowa z geometrią
2. Algebra w kryptografii
Wymagania wstępne:
1. Znajomość przestrzeni liniowych, ich bazy i wymiaru, przekształceń liniowych, macierzy, wyznaczników oraz rozwiązywania układów równań.
2. Znajomość zagadnień związanych z kongruencjami, ideałami pierścieni, pierścieniami ilorazowymi, ze szczególnym uwzględnieniem pierścieni wielomianów.
3. Posiadanie wiedzy na temat konstrukcji i najważniejszych własności ciał skończonych, w tym wielomianów minimalnych i pierwiastków z 1.

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Zdobycie wiedzy na temat wybranych metod kodowania i dekodowania liniowego nad dowolnym ciałem skończonym i poznanie jak zaawansowane narzędzia algebraiczne pozwalają rozwiązywać praktyczne problemy w teorii kodowania.

**Treści kształcenia:**

1. Kodowanie w sieciach. Idea modulacji i detekcji.
2. Kody liniowe nad dowolnymi ciałami skończonymi. Ogólne metody kodowania i dekodowania. Kody dualne. Wielkość kodów liniowych.
3. Wybrane metody konstrukcji kodów.
4. Kody doskonałe, ich parametry i związki z kombinatoryką. Kody Hamminga i kody Golay’a.
5. Kody cykliczne jako ideały w odpowiednich pierścieniach ilorazowych. Zera kodów cyklicznych.
6. Kody BCH - kody poprawiające błędy wielokrotne. Binarne kody BCH i metody ich dekodowania - wielomian lokalizacji.
7. Niebinarne kody Reeda-Solomona.
8. Kody liniowe z maksymalną odległością (rozszerzone kody RS). Cykliczne kody MDS.
9. Kody reszt kwadratowych. Dekodowanie permutacyjne.
10. Kody alternujące. Uogólnione kody RS.
11. Kody Goppa w kryptografii. System McEliece z kluczem publicznym.

**Metody oceny:**

Ocena z przedmiotu wystawiona będzie na podstawie punktów uzyskanych z dwóch kolokwiów (maksymalnie po 20 pkt. za każde kolokwium) oraz aktywności na zajęciach – maksymalnie 20 pkt. Zdobycie w sumie 31 punktów oznacza zaliczenie ćwiczeń i wykładu.

**Egzamin:**

nie

**Literatura:**

1. pod red. A. Dąbrowski, P. Dymarski, Podstawy transmisji cyfrowej, Oficyna Wydawnicza PW, 2004.
2. R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 2012.
3. J.H. van Lint, Introduction to Coding Theory, Springer, 1999.
4. W. Lipski, W. Marek, Analiza kombinatoryczna, PWN, Warszawa, 1986.
5. A. Pilitowska, Algebraiczne aspekty teorii kodów, preskrypt Oficyna Wydawnicza PW, 2019.
6. V.Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1982.
7. N.J.A.Sloane, F.J. MacWilliams, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

**Witryna www przedmiotu:**

brak

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka KKO\_W01:**

Zna ogólne zasady określające kodowanie z informacją nadmiarową.

Weryfikacja:

kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2\_W03, M2\_W01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka KKO\_W02:**

Zna algorytmy kodowania i dekodowania dla wybranych kodów liniowych nad ciałami skończonymi.

Weryfikacja:

kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2\_W03, M2MCB\_W01, M2MCB\_W03

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka KKO\_U01:**

Posiada umiejętność posługiwania się algorytmami kodującymi i dekodującymi dla wybranych kodów liniowych.

Weryfikacja:

kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2MCB\_U02, M2MCB\_U03, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

**Charakterystyka KKO\_U02:**

Posiada umiejętność zastosowania kodów korekcyjnych do szyfrowania przesyłanej informacji.

Weryfikacja:

kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka KKO\_K01:**

Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w teorii kodowania informacji.

Weryfikacja:

samoocena

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**